雙月刊
遠矚高瞻，穩步前行。

清流

No.51
2024.05 月號

洞悉「矽盾」護國盲點
培力產業引流之力

兩強之間難為小？
試看蒙庫特與朱拉隆功的借鑑

非自願獨身者運動
之發展與進化

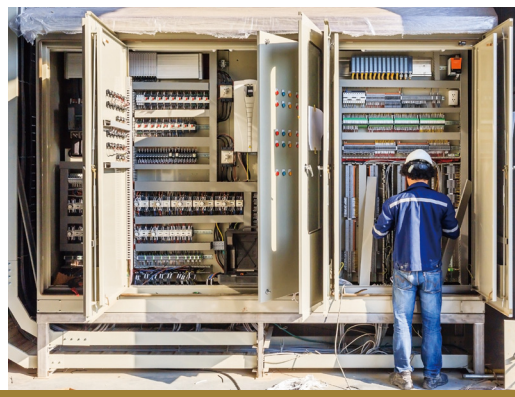
科技之島 站穩國際
臺灣「矽盾」再進化

法務部調查局　編印

雙月刊 2024.5月號 NO.51

清流 MJIB

目錄



封面
NO.51 MAY 2024

發 行 人：王俊力
副發行人：孫承一、吳富梅、吳以公、余尚賢
社　　長：凌文興
副 社 長：許銘侑
主　　編：蕭朝姓、黃日萱
文字編輯：朱美音、張堯明
出 版 者：清流雜誌社
發 行 所：法務部調查局
社　　址：新北市新店區中華路 74 號
e-mail：2d40@mjib.gov.tw
法律顧問：劉紀翔律師
美編印刷：加斌有限公司
地　　址：臺北市大安區復興南路二段 210 巷 30 號 1 樓
電　　話：（02）2325-5500
每本工本費新臺幣 30.8 元

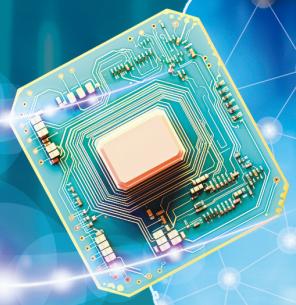
歡迎點閱電子書
http://www.mjib.gov.tw

GPN: 2010500577
ISSN: 2415-4970

中華郵政板橋雜字第 224 號登記證
登記為雜誌交寄

掃描 QR Code 閱覽電子書版本，可快速連結至其他資料來源，閱讀更多資訊！

科技之島 站穩國際



2024 年台積電進駐日本九州，
拓展矽盾實力並增進盟友鍊結。
美中科技貿易戰持續熱化，
誰掌握先端科技，就搶占致勝先機；
在這世界競逐賽中，臺灣應如何布局，
才能凸顯自身利基而不被各方勢力掣肘；
而在科技業奔馳的同時，
其他領域如何內化轉型，
均值吾人深思。

洞悉「矽盾」護國盲點 培力產業引流之力

◆ 中興大學國際政治研究所教授 — 譚偉恩

半導體產業是臺灣的矽盾，然而，中國大陸已在試圖減少其對臺灣晶片的依賴程度；同時，歐美國家也在設法淡化臺灣半導體產業在全球供應鏈中的角色。對此，我們有必要看清「矽盾」之說的盲點，在產業發展方向和國安策略上做出適時調整。

透過晶片與全世界緊密交織

何種因素的存在或哪些條件的具備能讓臺灣的自主獨立性免於對岸的染指？模糊的戰略同盟和常態化之軍備採購或許在一定程度上發揮了嚇阻中共武犯臺灣之念想，但我們都知道單憑這樣的同盟關係和武器質量不足以保證臺灣的生存安全。眼下臺灣必須極至善用手上的一項優勢—半導體產業：驅動當前全球經濟活動的主幹—來提高中共對臺發動軍事侵略的經濟成本，[1] 並加強歐美國家在兩岸不幸爆發軍事衝突後立即介入之意願。這當然不是一件容易的事，但卻是身為科技島的臺灣非做到不可之事。

[1] 此為「矽盾」之說的原始核心概念，由 Craig Addison 在 2000 年提出，他認為臺灣可利用自己在全球數位經濟上關鍵供應者的角色來嚇阻中共的軍事侵略。詳見：Craig Addison, *Silicon Shield: Taiwan's Protection Against Chinese Attack*, Fusion Press, 2001。

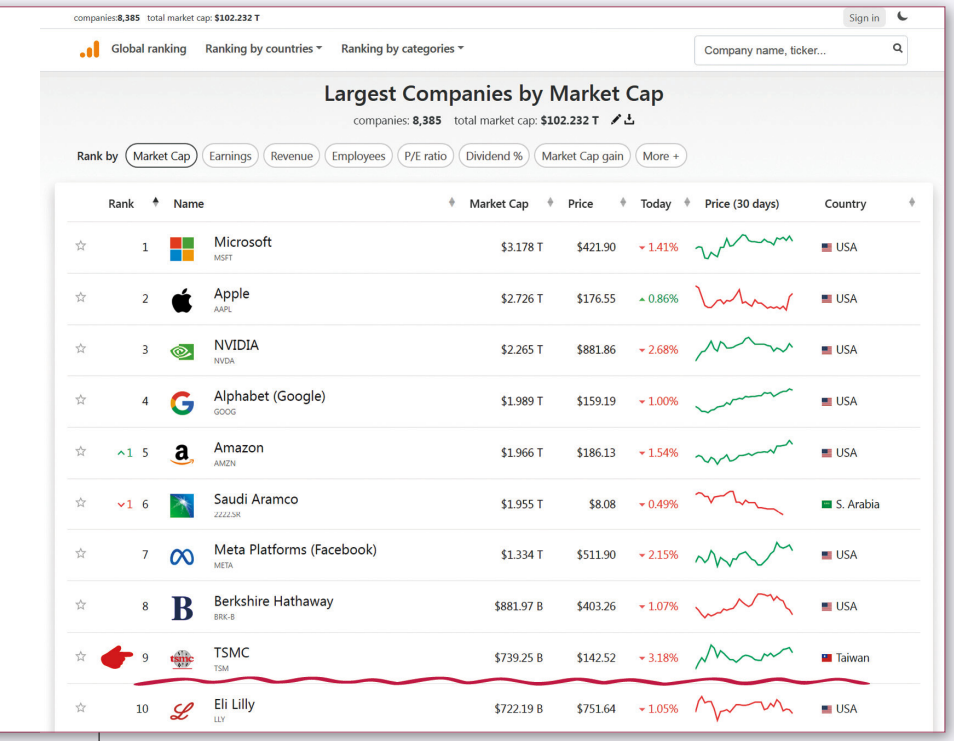
現代人生活上的許多用品，尤其是使用到電力的設備，大多都會用上晶片，因此晶片在研發及生產上的重要性已被許多國家納入安全戰略的一環。

隨著第五代行動通訊技術（5G）、物聯網（IoT）、區塊鏈等前沿科技與一國競爭力之關聯性日益緊密外，作為高科技產品核心的微處理器晶片（microprocessor chips）在研發及生產上的重要性已被許多國家納入安全戰略之一環。台灣積體電路製造股份有限公司（TSMC）目前是全球最大的晶片代工廠，但它的關鍵地位不僅止於全球科技市場上的經濟面向，還包括美中兩強已持續數年的國際地位之爭，以及晶片的研發和使用如何左右下一個十年（至少）各國的興衰。

TSMC 在全球晶片供應鏈中占有非常重要的地位，而這樣的地位在美中戰略競爭加劇之際，絕對不能被中國大陸掌握或破壞，否則美國目前享有之優勢可能瞬間就被中國大陸超越。詳言之，由於 TSMC 在先進晶片的製造水平遠遠領先它的同業，因此如果中共能藉由武力犯臺來掌控 TSMC，中共無疑將獲得一個重要的議價籌碼，並使其原本在國際稀土市場上擁有的影響力更加顯著。對臺灣來說，1987 年 TSMC 成立時，因為獲得之投資金額有限，初始營運並不被看好；但當時政府挹注約 22 億的發展基金，並對半導體產業給予能源使用上的補貼和便利，造就今天 TSMC 成為全球最大的晶片製造商和世界第九大市值的企業。[2] 對國際投資者而言，若 TSMC 陷入中共之手，經濟上的損失極可能是難以承受之重；[3] 國際投資者目前大約持有該公司 78% 左右的股份，如果兩岸發生軍事衝突，尤其是 TSMC 受到戰火牽連，全球經貿市場必然會有一連串之連鎖反應。

[2] Robert Wade, *Governing the Market: Economic Theory and the Role of Government in East Asian Industrialization*, Princeton University Press, 1990, Ch. 4；瞿宛文，〈護國神山的由來：當年的台積電，是如何在一片質疑中被催生出來？〉，《獨立評論》，2023 年 3 月 15 日，https://opinion.cw.com.tw/blog/profile/390/article/13390。

[3] 蘋果、輝達、高通和超微半導體公司（AMD）等 TSMC 的客戶以及 ASML 和科磊（KLA-Tencor）等 TSMC 的設備供應商將受到嚴重影響。



根據全球上市公司市值排行網站 Companies Market Cap 的統計，台積電是世界排名第九大市值的企業。（Source: Companies Market Cap, https://companiesmarketcap.com）

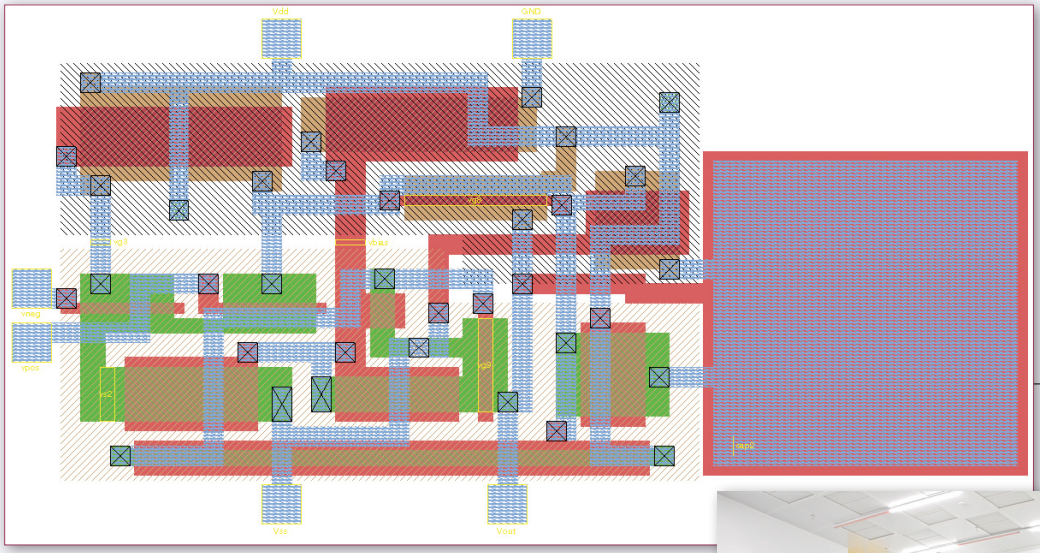
儘管目前最先進的半導體製造設備是由歐洲和美國提供的，但 TSMC 是全球最大的合約晶片製造商，生產近 90% 用於人工智慧和量子運算所需之尖端晶片。簡言之，沒有其他製造商能夠像 TSMC 一樣大規模地生產質優又複雜的高端晶片。正因為如此，TSMC 成為一個地緣政治與地緣經濟的重要行為者，不僅讓臺灣與世界鏈結，也讓世界的半導體產業離不開臺灣。舉例來說，美國在先進晶片的積體電路布局設計和半導體相關設備的研發上，處於全球龍頭地位；臺灣是擁有全球最先進半體體製程的代工廠，並在組裝、封裝和測試方面居於領先；而荷蘭的艾司摩爾（ASML）則是國際上唯一有能力製造高數值孔徑極紫外光（High NA EUV）光刻機的公司。美臺荷三方是相互依賴，唇齒相依。

隨著晶片的應用從工業拓展到日常生活的諸多方面，甚至成為新型服務產業的好幫手，半導體產業已是人類社會未來經濟活動的基石。在這樣的脈絡之下，如果臺灣的半導體產業在中共武力犯臺時被迫中斷生產，全球晶片的需求將瞬間萎縮，隨之而來的經濟衝擊無疑是災難性的，這也是為何關注經濟成長與技術創新的歐美國家或新興經濟體會對臺海現狀是否穩定至為關切，「矽盾」的說法在相當程度上也是由此而生。

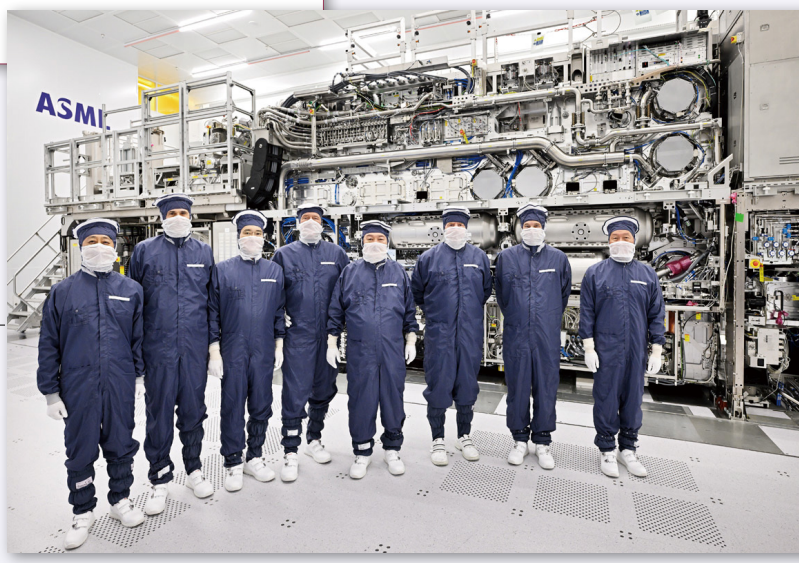
「矽盾」護臺論的盲點

如果中共當局試圖以武力來解決臺灣的主權歸屬，並藉機順勢掌握 TSMC，必然會是一個風險甚鉅之決定（即便可能不是非理性的選擇）。[4] 因為就算其能在短期內成功占領臺灣，美國和它在世界各地的盟友也會以無預設底限的時間來對中共進行各種抵制，就像此時戰火仍未停歇的俄烏衝突。超級強權間的競爭在本質上偏向零和賽局，一旦開啟幾乎很難不陷入安全

[4] John Mearsheimer and Sebastian Rosato, *How States Think: The Rationality of Foreign Policy*, Yale University Press, 2023, x-xiii.



美國擁有良好的技術和研發能力，在先進晶片的積體電路布局設計和半導體相關設備的研發上，處於全球龍頭地位。（Photo Credit: Atropos235, https://w.wiki/9nLn）



荷蘭的艾司摩爾公司是國際上唯一有能力製造高數值孔徑極紫外光光刻機的公司，是現代積體電路不可或缺的重要供應商；圖為韓國政府參訪 ASML 的畫面。（Photo Credit: Ministerie van Buitenlandse Zaken, https://flic.kr/p/2pFYqm3）

困境；任何一方守勢性的作為都很容易被另一方解讀為具有針對自己的攻勢意圖。在此情況下，即使臺灣主權爭議和 TSMC 不存在，美中之間的結構性衝突也同樣難以避免。

有鑑於此，如果中國大陸的決策者是理性的，應該要到萬不得已之際才會選擇用軍事手段來作為「回應」。這也就是說，對臺使用武力應該是「被動的選擇」，而非「主動的選項」；因此，嚇阻中共對臺軍事侵略的關鍵原因是美中當前已白熱化的權力較勁，以及還未改變臺海現狀的臺灣，並不是 TSMC 或所謂的「矽盾」。然而，如果加上對全球經濟至關重要的臺灣半導體產業之後，會不會形成對中共更穩健的嚇阻效果呢？本文的愚見是「未來不會」，因為 TSMC 的重要性已成為一個地緣政治與地緣經濟議題，讓歐美國家意識到自己對 TSMC 所生產之晶片的高度依賴。出於自主性及經濟安全的考量，歐美國家紛紛開始投入半導體生產「本土化」，但由於半導體是頂尖的科技產品，製程複雜，資金與技術需求極高，即便是歐美先進工業國家也要數年的時間才有可能不再仰賴 TSMC。正因為如此，美國國務卿 Blinken 在 2023 年表示，美國尋求維護臺海和平暨穩定，認為這是符合所有國家利益的情況。基於臺灣海峽每天約有全球商業一半

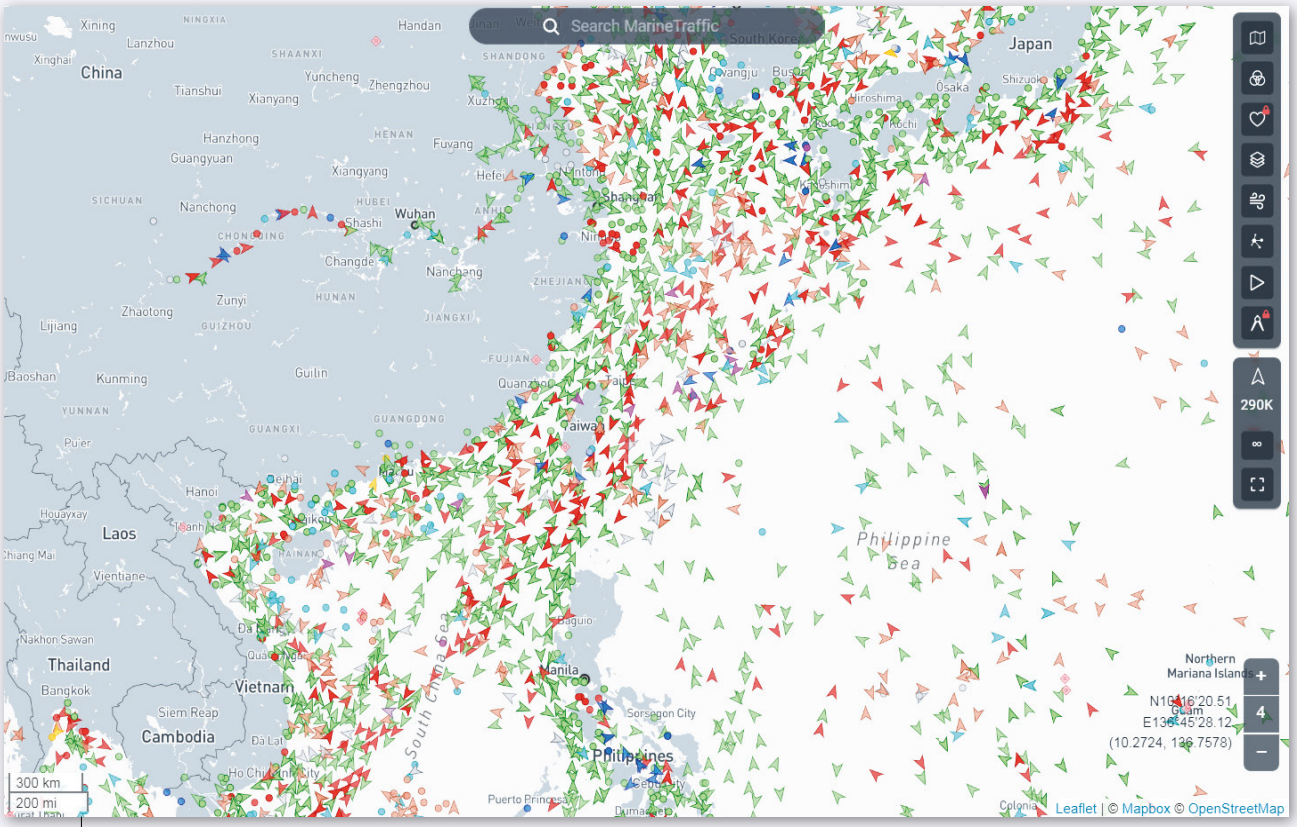
俄羅斯總統普丁無視西方國家的各種制裁與抵制，於 2022 年 2 月 24 日宣布進行「特別軍事行動」，對烏克蘭發動全面入侵，兩方交戰至今，造成了嚴重死傷，以及歐洲自第二次世界大戰以來最大的難民危機。（Photo Credit: ДСНС України, https://www.facebook.com/photo?fbid=682526567248569; МВС України, https://www.facebook.com/photo/?fbid=321830783305911）

以上的船隻經過，世界上大約 70% 的半導體是臺灣直接或間接製造的，美國反對臺海任何一方片面改變目前的情況。

上述 Blinken 的觀點在某程度上證成了「矽盾」之說，但其中的盲點卻不易為人覺查。即便「矽盾」之說現在屬實，生活在臺灣的我們也不可因此認為國家安全會一直無虞。我們必須盡快讓臺灣的半導體產業吸引更多外國行為者（從國家、企業到個人）加入在臺灣當地的設計、研發及製造過程。這樣臺灣的半導體產業才是真正從裡到外和由外至內的國際化；既有輸出，亦有引入。而引入的資金和人才就是臺灣這個科技島的一部分，特別是那些來到臺灣的外國科技菁英會和我們一起工作及生活，甚至會在臺灣落地生根，如此臺灣的生存安全便與這些人緊扣，彼此依存，同島一命！

「矽盾」再進化

臺灣自 1949 年以來一直都在為人民解放軍可能的軍事侵襲做準備。2020 年以前，兩岸之間還有經貿互賴可以作為抑制衝突爆發之舒緩劑，但現在貿易和平論的效用明顯降低了，[5] 反而是臺灣半導體產業在全球供應鏈中的關鍵地位讓中共對武犯臺灣這個選項投鼠忌器。持平而論，儘管不是一個民主政體，中共對於經濟發展的重視並不亞於民主國家的政府，當無以計數的經濟活動及其相關物件或



從船舶公開資訊網站 Marine Traffic 的即時地圖可以看到，臺灣海峽與臺灣東部皆是非常繁忙的航道，同一時間有許多貨船（綠點）與油輪（紅點）經過，因此臺灣海峽的和平穩定對全球供應鏈至關重要。（Source: Marine Traffic, https://www.marinetraffic.com/en/ais/home/centerx:121.5/centery:23.3/zoom:7）

設備皆不能沒有晶片時，確保半導體在國際間供應鏈的安全就成為中共治國戰略中的優先要務，這點對於大權在握的習近平也不例外。

對臺灣這個科技島而言，我們必須緊緊握住目前手中持有的晶片生產優勢，但同時將臺灣的利益緊緊地與美國及其盟邦的利益交織在一起。如此中共鬧事，臺灣有事，就必然是國際大事。至於在兩岸沒有開打之前，臺灣必須做好準備，阻止中共以「非武力的方式」奪取我們半導體產

臺灣的半導體產業應吸引更多外國人才加入，方能達成由外至內的國際化，讓引入的資金和人才成為臺灣的一部分，如此臺灣的生存安全便與這些人緊扣，彼此依存，同島一命！

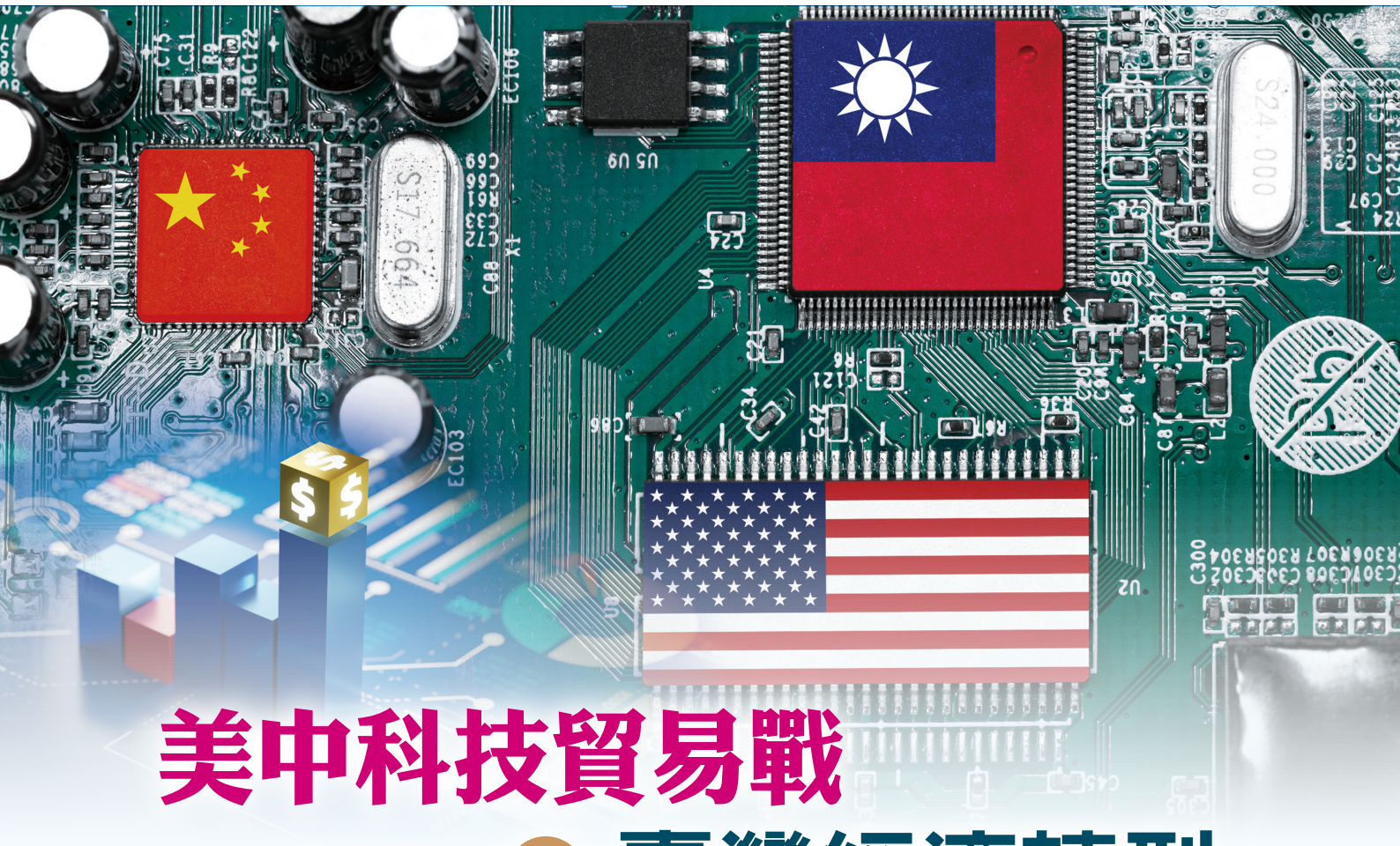
[5] Bonnie Glaser and Jeremy Mark, "Taiwan and China Are Locked in Economic Co-Dependence," *Foreign Policy,* April 14, 2021, https://foreignpolicy.com/2021/04/14/taiwan-china-econonomic-codependence/; Benjamin Schreer, "The Double-Edged Sword of Coercion: Cross-Strait Relations After the 2016 Taiwan Elections," *Asian Politics & Policy*, Vol. 9, No. 1, 2017, pp.50-65.

大陸的行動支付使用非常普遍，幾乎已讓中國成為了無現金社會，而使用行動支付的相關設備皆脫離不了晶片，因此確保半導體供應鏈的安全就成為中共治國戰略中的優先要務。（Photo Credit: Shwangtianyuan, https://w.wiki/9nPL; Enviro2800, https://w.wiki/9nPM）

業的控制權。[6] 舉例來說，全力防止 TSMC（還有其他臺灣的晶片製造公司）被陸籍企業或與中國大陸有關係的企業惡意收購。這方面需要採取良好的監管和政策來應對，並以協助臺灣業者的立場來執行相關法令。本文拙見以為，防止中資惡意收購 TSMC 的方法是立法院授予主管半導體產業的政府部門有權對試圖收購 TSMC（或其他臺灣晶片製造業者）的行為者進行實質資格審查及否決權。實務上可以參考英國政府對該國汽車業者 Rolls-Royce 的保護措施，即限制非英國籍的投資者持有該公司一定比例以上的股份。

臺灣半導體產業在全球供應鏈中的關鍵地位給了我們一個契機，可以用以說服美國有必要保護臺灣才能防止中共在競爭過程中超越美國。另一方面，臺灣有必要讓中共知道，即使解放軍能夠掌控臺灣半導體並取得相關技術，那也只是全球半導體供應鏈中的一環而非全部；因此，一旦美國及其盟友在供應鏈上游與臺灣的合作關係會隨著臺海戰事的爆發而中斷，其影響必將導致中國大陸所需的晶片面臨短缺，這對目前經濟治理面臨嚴重困境的習近平來說，絕對是雪上加霜，弊大於利。

[6] 2015 年北京的清華紫光集團入股我們臺灣的力成科技，並試圖進一步取得矽品與南茂兩間公司各 25% 左右的股權。此事件由於立法院和經濟部投審會當時審查嚴謹，最終才未讓紫光集團如願。值得留心的是，此事件後續發展也確實與我國審查結果呼應，紫光集團因不當商業行為在 2021 年 7 月破產，集團董事長諸多違法行徑被舉報。參考：〈債務危機延燒！中國紫光遭徵銀聲請破產重整〉，《財訊》，2021 年 7 月 10 日，https://www.wealth.com.tw/articles/59c78fa5-85d6-4a53-a19d-e7ac2793ad6f。



美中科技貿易戰與臺灣經濟轉型

◆ 中華經濟研究院第一研究所助研究員 — 王國臣

美中經貿戰持續升溫，美國藉商業、投資、技術研發等管制，對大陸軍事、半導體、關鍵技術等領域多方制衡，同時積極對外鞏固先進科技及原物料之領導聯盟；臺灣雖得以更鞏固臺美關係，但內部經濟與薪資結構失衡擴大的貧富差距，以及被全球通膨推升的物價，對總體經濟發展仍存挑戰，宜儘速規劃長遠戰略。

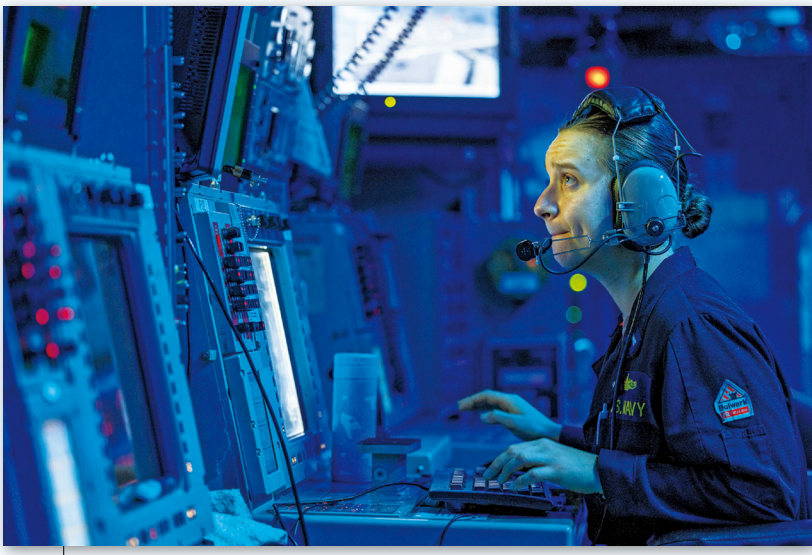
美中科技貿易戰

美國貿易代表辦公室（United States Trade Representative, USTR）2018 年啟動第一波貿易制裁，至 2024 年 2 月，華府累計對陸輸美之 6,842 項商品（價值 2,500 億美元），加徵達 25% 之懲罰性關稅；另對 1,120 億美元的陸製商品加徵 7.5% 關稅。前總統川普曾坦言是針對「中國製造 2025」。2018 年 7 月美國通過《外國投資風險審查現代化法案》（*Foreign Investment Risk Review Modernization Act*, FIRRMA），擴大海外投資委員會（Commit-

「中國製造 2025」是前任中國國務院總理李克強提出的製造業政策，也是中國政府實施「製造強國」戰略的首個十年綱領；目標是中華人民共和國成立一百年時，把中國建設為引領世界製造業發展的製造強國。

tee on Foreign Investment in the United States, CFIUS）的審查權限，含括具備關鍵技術、28 個領域的重要基礎設施，以及 11 類敏感個資等美國企業（統稱為 TID 企業），戰火旋即延燒到科技領域。

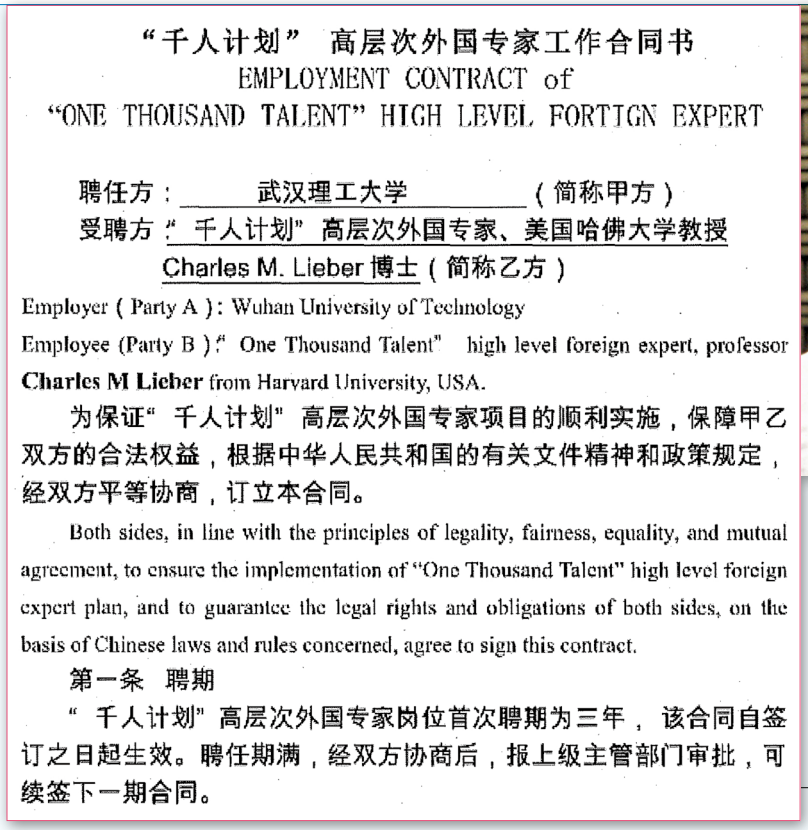
CFIUS 並未列舉關鍵技術清單，而是轉由商務部工業和安全局（Bureau of Industry and Security, BIS）負責。準此，BIS 歷經 7 次增修《出口管制條例》（*Export Administration Regulations*, EAR），累計限制 31 項新興技術，更緊縮軍用企業（Military End User, MEU）管制，品項亦延伸到軍事相關的半導體設備、電信設備與技術。華府同時間修增最低門檻境外製造比率至 90%，並擴大外國直接產品原則（Foreign Direct Product Rule）的涵蓋範圍，另新增中共涉軍企業（Communist Chinese Military Companies, CCMC）與中共軍工複合體公司（Non-SDN Chinese Military-Industrial Complex Company, NS-CMIC）兩份清單，禁止美國民眾投資相關企業，遏制中國大陸軍事技術研發。



BIS 限制美國軍事相關的半導體設備、電信設備與技術之出口，以此遏制中國大陸軍事技術的研發。（Photo Credit: U.S. D.O.D, photo by Hannah Fry, https://www.defense.gov/Multimedia/Photos/igphoto/2003421644/）

美國司法部 2018 年起也推展中國專案（China Initiative），鎖定中國大陸竊密行為。2024 年 2 月底，聯邦調查局共起訴 156 名駭客與商業間諜，其中多人涉及「千人計畫」，美國並陸續限制中共官員、解放軍、陸籍理工學生、國有企業主管與科技公司職工赴美簽證。同時期，CFIUS 共否決 44 起中國大陸企業赴美直接投資與跨國併購案；BIS 亦框列 723 家陸商至出口管制實體清單，並將 39 家廠商納入未經核實清單（Unverified List, UVL）；CCMC 與 NS-CMIC 則更擴增到 144 家。

美國還推動經濟繁榮網路（Economic Prosperity Network, EPN）的夥伴聯盟，發起乾淨網路（clean network），檢視電信設備商涉中程度。隨後推出《印度—太平洋經濟框架》（*Indo-Pacific Economic Framework for Prosperity*, IPEF），邀集臺灣、日本與韓國，組建晶片四方聯盟（Chip



“千人计划” 高层次外国专家工作合同书
EMPLOYMENT CONTRACT of
“ONE THOUSAND TALENT” HIGH LEVEL FORTIGN EXPERT

聘任方：武汉理工大学（简称甲方）
受聘方：“千人计划”高层次外国专家、美国哈佛大学教授
Charles M. Lieber 博士（简称乙方）

Employer (Party A): Wuhan University of Technology
Employee (Party B): “One Thousand Talent” high level foreign expert, professor **Charles M Lieber** from Harvard University, USA.

为保证“千人计划”高层次外国专家项目的顺利实施，保障甲乙双方的合法权益，根据中华人民共和国的有关文件精神和政策规定，经双方平等协商，订立本合同。

Both sides, in line with the principles of legality, fairness, equality, and mutual agreement, to ensure the implementation of “One Thousand Talent” high level foreign expert plan, and to guarantee the legal rights and obligations of both sides, on the basis of Chinese laws and rules concerned, agree to sign this contract.

第一条　聘期

“千人计划”高层次外国专家岗位首次聘期为三年，该合同自签订之日起生效。聘任期满，经双方协商后，报上级主管部门审批，可续签下一期合同。

「千人計畫」是中共招攬海外人才的計畫，美國國情會指出其動機是「促進以合法和非法方式，將美國的技術、智慧財產權和專有技術轉移及輸送給中國」；前哈佛大學教授 Charles Lieber 隱瞞參與，作出虛假陳述並提交虛假納稅申報，於 2021 年因「中國專案」被定罪。（Source: U.S. Department of Justice, https://www.justice.gov/opa/press-release/file/1239796/dl; Kris Snibbe, https://w.wiki/9mub）

4 或 Fab 4），且加強友岸外包（Friend-shoring），* 提升供應鏈韌性。此外，持續布局藍色太平洋夥伴（Partners in the Blue Pacific, PBP）、撒哈拉以南非洲，並加入亞得里亞海—黑海—波羅的海的三海合作，以及攜手七大工業國集團（Group of Seven, G7）共同發布《重建更好世界》（*Build Back Better World*, B3W）倡議，計劃向開發中國家投入 40 兆美元，確保關鍵礦物供給。

臺灣國際經貿布局的挑戰

美中科技貿易戰，解構行之多年的三角貿易，臺灣對美出口占比由 2017 年的 11.7%，攀升到 2023 年的 17.6%，也使在陸臺商相繼返臺。目前美國是臺灣第二大出口國，較 2017 年前進 1 位。美國自臺灣進口占比，亦由 1.8% 拉升到 2.8%；臺灣躍居美國第八大貿易夥伴，較 2017 年進步 5 名（見下頁圖 1）。

2023 年 6 月《美臺 21 世紀貿易倡議》（*U.S.-Taiwan Initiative on 21st-Century Trade*）第一階段達成，涉及貿易便捷化、服務業規章與中小企業，並將延伸到農業、勞工權益、數位貿易、國營事業、非市場政策、標準對接與環境議題；在此之際，中國大陸加速不可靠實體清單、出口管制、數據出境與網路安全等科技相關領域的單邊立法，其中包含《阻斷外國法律與措施不當域外適用辦法》，即臺灣企業如因應美國出口管制而拒絕出貨，則中國大陸可逕行裁罰。臺廠為順應美國高水平的經貿條件，生產成本勢必墊高，而大陸的單邊立法，則可能讓臺商由左右逢源轉向腹背受敵。（見下頁表 1）

* 為美國實施的一項外交及貿易政策，旨在要求企業撤離與美國有地緣政治衝突的國家，轉而優先與盟國或價值觀相近的國家發展貿易關係，並建立彼此互助的供應鏈，也稱友岸合作。

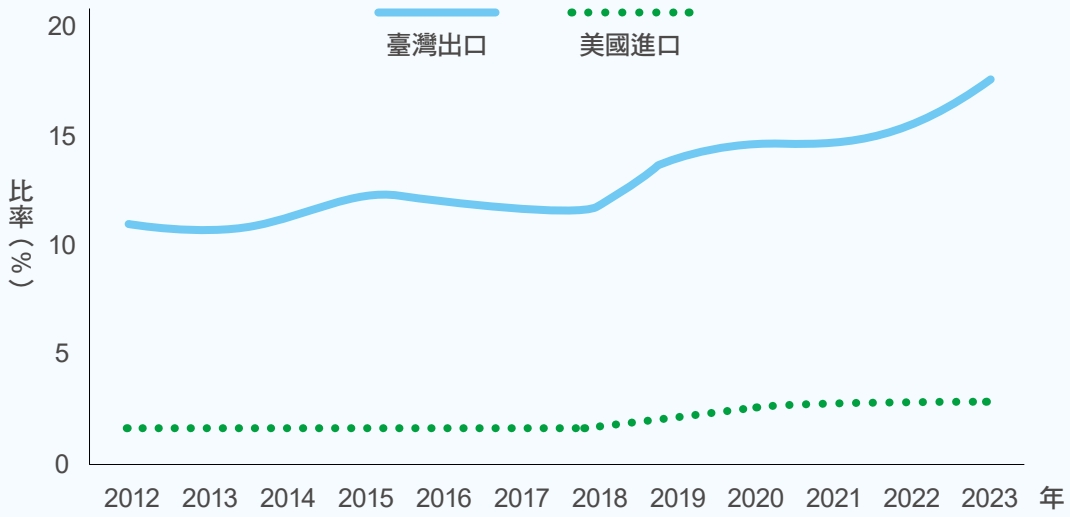


圖 1　臺灣與美國雙邊貨物貿易

表 1　中國大陸國際經貿制裁單邊立法

時間	發布單位	法規名稱
2019/5	商務部	不可靠實體清單規定
2020/8	商務部暨科技部	禁止與限制出口技術目錄
2020/10	全國人民代表大會常務委員會	出口管制法
2020/11	國家發展和改革委員會	外商投資安全審查辦法
2020/12	商務部暨海關總署	兩用物項和技術進出口許可證管理目錄
2021/1	商務部	阻斷外國法律與措施不當域外適用辦法
2021/6	全國人民代表大會常務委員會	反外國制裁法
2021/6	全國人民代表大會常務委員會	數據安全法
2021/8	國務院	關鍵數據基礎設施安全保護條例
2022/1	國家互聯網信息辦公室	網路安全審查辦法
2022/7	國家互聯網信息辦公室	數據出境安全評估辦法
2023/2	證券監督管理委員會	境內企業境外發行證券和上市管理試行辦法
2023/4	全國人民代表大會常務委員會	反間諜法
2023/9	全國人民代表大會常務委員會	外國國家豁免法
2024/2	全國人民代表大會常務委員會	保守國家秘密法

資料來源：作者自行整理。

此外，世界先進國家更相繼投入半導體競賽，以韓國最為積極，預計 10 年內投入 510 兆韓元（折合 4,665 億美元）；英國與中國大陸則緊追在後。歐盟、日本、美國、法國與德國亦斥資百億美元。臺灣晶創計畫於 2024 年甫開始實施，且規模僅 96 億美元，恐衝擊「護國神山」與矽盾（silicon shield）的發展。（表 2）

表 2　世界先進國家半導體產業研發計畫

國家	時間	計畫	億元	億美元
韓國	2024 年	K 半導體戰略	6,220,000	4,665
英國	2024 年	半導體研發計畫	3,500	4,445
中國大陸	2021 年	十四五年規劃	20,000	2,800
歐盟	2023 年	歐洲晶片法案	430	469
日本	2021 年	半導體與數位產業戰略	33,550	225
美國	2022 年	晶片與科學法案	390	390
法國	2022 年	電子 2030 計畫	300	327
德國	2023 年	氣候與轉型基金	200	218
臺灣	2024 年	晶創計畫	3,000	96

說明：元表示該國本幣計價；觀測時間截至 2024 年 3 月 17 日。

臺灣經濟結構的扭曲

全球對資通訊科技（Information and Communications Technology, ICT）產品的需求若渴，帶動臺灣出口擴張。ICT 外銷訂單占比，由 2018 年美中科技戰起的 29.0%，爬升到 2020 年的 30.8%，連續 3 年走揚，且創歷史新高（圖 2）。影響所及，經濟成長率飆升 3.8 個百分點至 6.6%。惟此後國際邁入去庫存，故 ICT 外銷訂單與經濟成長率，方逐步收斂。

問題是，臺灣 ICT 產業產值占比由 2019 年的 19.3%，上升到 2022 年的 22.4%，共增加 3.1 個百分點；其中，ICT 製造業產值占比增加，但排除 ICT 後的製造業產值占比則相應衰退。易言之，經濟結構過度依賴 ICT 單一產業，將加大景氣波動。（表 3）

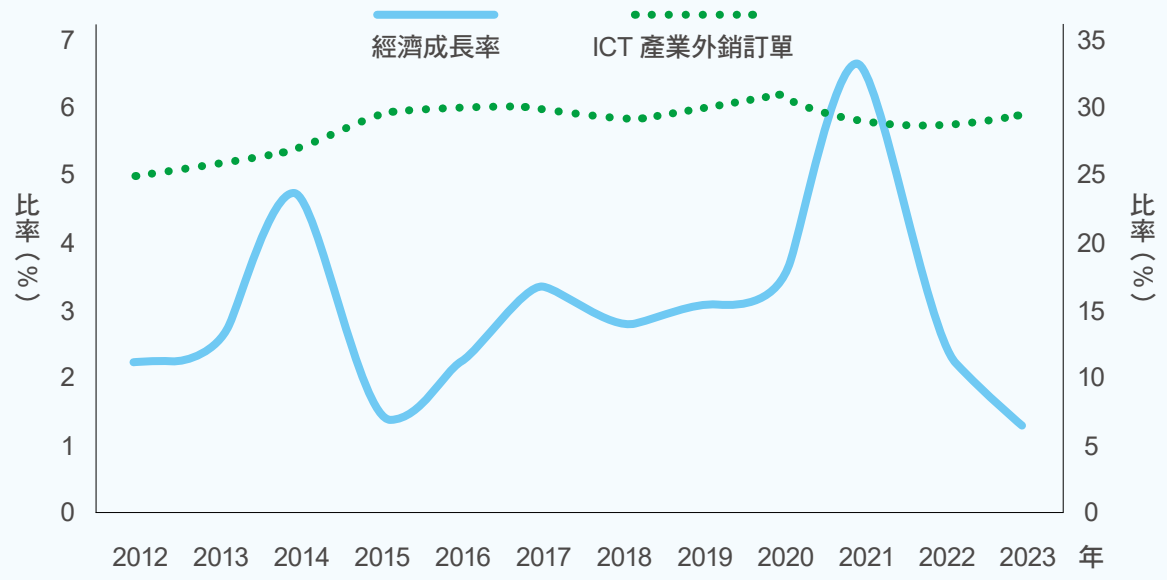


圖 2　臺灣經濟成長率與資通訊科技產品外銷訂單

經濟結構失衡亦加大貧富差距。每人可支配所得吉尼係數（Gini coefficient），由 2020 年的 27.4% 爬升到 2022 年的 27.9%，連續第二年攀升。其中，2022 年 ICT 製造業員工薪資為 94,719 元，較 2020 年明顯增加。ICT 服務業員工薪資，亦累計成長 9.2%。反之，非 ICT 製造業與服務業薪資，僅分別成長 7.2% 與 5.8%。（表 4）

更嚴峻的是，全球通貨膨脹推升臺灣物價，進口物價指數由 2020 年的 85.8 點，攀升到 2023 年的 100.6 點，累計上漲 17.3%。受此影響，消費者物價指數（Consumer Price Index, CPI）由 98.1 點攀升到 105.5 點，累計上漲 7.6%。信義房價指數亦由 115.2 點竄升到 153.4 點，累計上漲 33.2%。通膨將加劇非 ICT 產業員工的生計困難。（圖 3）

綜上述，受惠於科技持續創新，臺灣在全球 ICT 供應鏈的地位愈加鞏固，並推升經濟成長。惟產業結構過度集中，不僅放大景氣波動，尚加劇通膨與貧富差距。據此，非 ICT 產業員工生計更加艱困。故培育若干新成長點為政府當務之急；其中，尤以就業人口占 6 成的服務業為優先考量。

表 3　臺灣產業結構（依 ICT 區分）

單位：比率（%）

時間	ICT 產業			非 ICT 產業		
	合計	製造業	服務業	合計	製造業	服務業
2017 年	20.9	18.9	2.0	79.2	37.6	39.9
2018 年	19.3	17.5	1.9	77.0	39.0	40.2
2019 年	19.3	17.4	1.9	77.2	37.7	41.5
2020 年	21.5	19.6	2.0	76.2	35.5	41.5
2021 年	21.4	19.5	1.9	79.2	37.7	39.5
2022 年	22.4	20.5	1.9	77.0	36.6	39.7

說明：ICT 表示資通訊科技，含括電子零組件製造業、電腦電子產品及光學製品製造業、電信服務業，以及電腦相關與資訊服務業。

表 4　臺灣薪資結構（依 ICT 區分）

單位：元

時間	ICT 產業			非 ICT 產業		
	合計	製造業	服務業	合計	製造業	服務業
2017 年	71,795	74,124	69,466	48,261	48,989	47,532
2018 年	74,461	79,088	69,835	49,767	50,606	48,927
2019 年	76,730	81,596	71,863	50,837	51,440	50,234
2020 年	78,010	82,389	73,631	51,313	51,655	50,972
2021 年	82,809	90,432	75,186	52,423	53,115	51,732
2022 年	86,660	94,719	78,601	54,183	55,136	53,230

說明：ICT 表示資通訊科技，含括電子零組件製造業、電腦電子產品及光學製品製造業、電信服務業，以及電腦相關與資訊服務業。因薪資統計只列舉「出版、影音製作、傳播及資通訊服務業」，故本文以此替代 ICT 服務業。

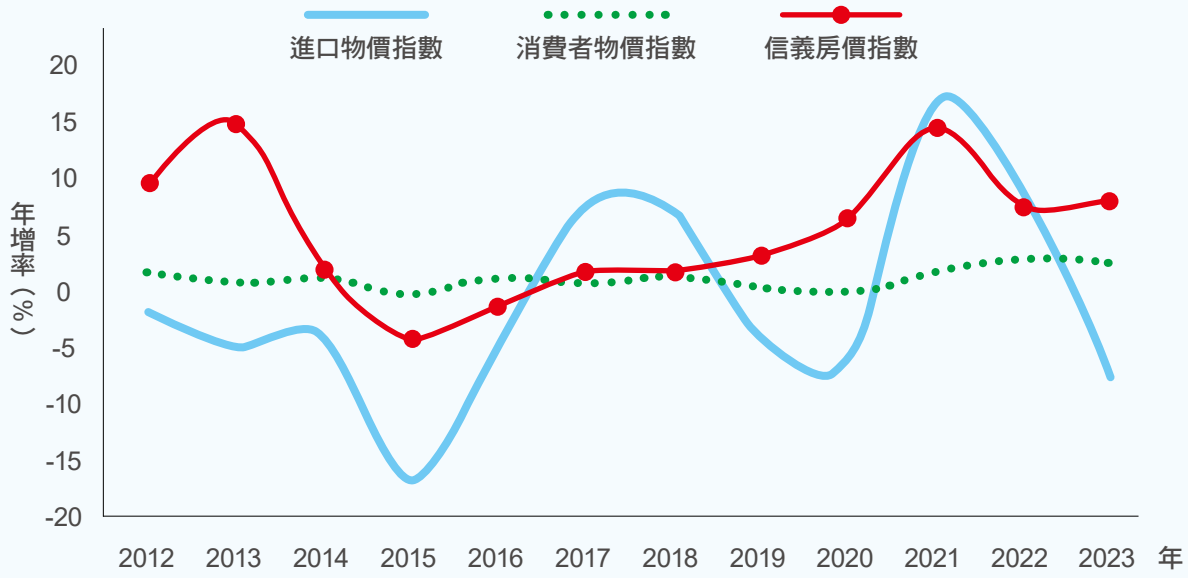


圖 3　臺灣物價走勢

結論

美中科技貿易戰重構全球供應鏈，並推升臺灣經濟成長，惟產業結構失衡，加大景氣波動、通膨與貧富差距。尤其是，為迎合臺美雙邊貿易的永續，臺商生產成本將逐步墊高。更嚴峻的是，各國競相投入半導體研發，疊加中國大陸單邊立法與新南向國家政治風險，皆制約臺灣產業國際布局。

尤其關注的是，地緣政治衝突更上升到標準設定。美國、日本、歐盟與中國大陸相繼發布標準化戰略。日本還於 2020 年邀集美國、加拿大、英國、歐盟、瑞典與瑞士共同研究央行數位貨幣（Central Bank Digital Currency, CBDC），G7 更研擬將數位人民幣（E-CNY），納入全球監管框架。易言之，全球科技競爭方興未艾。故繼美國於 2020 年發布《關鍵與新興技術國家戰略》（*National Strategy for Critical and Emerging Technologies*）後，日本也於 2022 年制訂《經濟安全保障推進法》。歐盟隨之跟進，於 2024 年發布《經濟安全戰略》（*European Economic Security Strategy*），慎防科技外流憂慮國家（countries of concern）。準此，臺灣也需加快擬定總體經濟安全戰略，並厚實國際合作。

儘管臺灣科技產業因為美中科技貿易戰而呈現榮景，推升經濟成長，但產業結構失衡的問題也日漸嚴重。（圖片來源：昇典影像，https://flic.kr/p/2m1NPMN）

美中科技戰與日本經濟安全戰略

◆ 國立臺灣師範大學東亞學系教授 — 林賢參

在一山不容二虎的邏輯下，兩虎相爭勢所必然。

一山不容二虎與「權力轉移」

美蘇兩極對立的 1950 年代末，探討美蘇兩虎爭霸的「權力轉移」（Power Transition）理論興起，惟因蘇聯的衰敗與瓦解而沉寂；中共崛起勢不可擋的 2000 年以降，權力轉移理論再度受到關注，特別是在對外獨斷專橫的中共總書記習近平政權執政後，描述新舊霸權之爭的「修昔底德陷阱」（Thucydides Trap）成為國際關係學界討論的焦點。經濟力乃是國力的主要來源，誠如提出霸權「長周期循環理論」（Long Cycle Theory）的美國學者孟德爾斯基（George Modelski）所言，在牽引世界經濟發展領域具有領先地位的「主導性經濟」（lead economy），乃是成為世界

2021 年 3 月，中共第十三屆全國人大第四次會議通過《國民經濟和社會發展第十四個五年規劃和 2035 年遠景目標綱要（草案）》的決議。（圖片來源：中新社／達志影像）

《國民經濟和社會發展第十四個五年規劃和 2035 年遠景目標綱要》中提出加強原創性、引領性科技之攻關，展現中共追求科技霸權的決心。

第二节　加强原创性引领性科技攻关

在事关国家安全和发展全局的基础核心领域，制定实施战略性科学计划和科学工程。瞄准人工智能、量子信息、集成电路、生命健康、脑科学、生物育种、空天科技、深地深海等前沿领域，实施一批具有前瞻性、战略性的国家重大科技项目。从国家急迫需要和长远需求出发，集中优势资源攻关新发突发传染病和生物安全风险防控、医药和医疗设备、关键元器件零部件和基础材料、油气勘探开发等领域关键核心技术。

专栏 2　科技前沿领域攻关

01　新一代人工智能
前沿基础理论突破，专用芯片研发，深度学习框架等开源算法平台构建，学习推理与决策、图像图形、语音视频、自然语言识别处理等领域创新。

02　量子信息
城域、城际、自由空间量子通信技术研发，通用量子计算原型机和实用化量子模拟机研制，量子精密测量技术突破。

03　集成电路
集成电路设计工具、重点装备和高纯靶材等关键材料研发，集成电路先进工艺和绝缘栅双极型晶体管（IGBT）、微机电系统（MEMS）等特色工艺突破，先进存储技术升级，碳化硅、氮化镓等宽禁带半导体发展。

04　脑科学与类脑研究
脑认知原理解析，脑介观神经联接图谱绘制，脑重大疾病机理与干预研究，儿童青少年脑智发育，类脑计算与脑机融合技术研发。

級霸權國的條件之一，而在當代國際舞臺上掌握「軍民兩用」（Dual-use）的新高科技，更是成為霸權國不可或缺的關鍵。

《中國製造 2025》引爆美中貿易戰與科技戰

中共國務院於 2015 年 3 月通過《中國製造 2025》推動方案，揭櫫今後十年重點發展的 10 項新高科技產業，希望透過對戰略性產業進行投資或補貼，以期掌握軍民兩用新高科技。惟此等產業發展計畫，被美國川普政府視為不公平貿易措施，因而在 2018 年對該等產業展開高關稅的貿易戰，再於翌年升級為科技戰。值此之際，習近平於 2020 年 10 月提示給國務院研擬第 14 個 5 年計畫的建議案中，依然要求寫入打勝在「人工智能」（AI）、量子、太空等新高科技領域的攻堅任務等字眼，展現中共追求科技霸權的決心。

美國智庫「外交關係協會」（Council on Foreign Relations, CFR）研究員拉斯凱（Lorand Laskai）撰文指出，《中國製造 2025》方案凸顯出中共違反「世界貿易組織」（World Trade Organization, WTO）的自由市場機制與規範，企圖透過收購、強制外國企業技術轉移、駭客竊取技術，以實現習近平的「中國夢」願景。拉斯凱在另一篇文章中強調，習近平的願景是透過民營企業參與國防科技發展的「軍民融合」政策，企圖將共軍打造為「世

界級戰鬥力量」，讓《中國製造 2025》成為美國技術領先的主要挑戰。簡言之，美中科技戰的本質，是爭奪 21 世紀科技產業的主導權，更是權力轉移過程中誰能勝出的關鍵。

面對中共崛起的挑戰，拜登政府不但延續川普的對中貿易戰、科技戰，其攻擊火力更加猛烈。拜登於 2022 年 8 月 9 日，簽署重振美國半導體產業的《2022 年晶片和科技法案》，並且據此於 9 月 6 日宣布，禁止接受過聯邦政府資金補助的美國公司在中國大陸擁有「先進技術」的工廠後，再於翌年 8 月 9 日發布命令，禁止美國企業與個人投資大陸（包括港澳）半導體、量子計算、AI 等三大新高科技領域，藉以阻斷中共取得美國新高科技的管道。在美中科技戰場上，拜登政府揚棄川普的美國優先路線，改採重視與同盟友邦合作，而日本就成為美國對中科技戰的最重要盟邦之一。

日本政府修法並創設確保經濟安全部門

日本政府為配合美國對中科技戰，以及因應中共的經濟脅迫，除了著手進行修法與立法之外，也建構雙邊與多邊機制，以期建構將經濟與國家安全結合一體、特別是強化供應鏈韌性與產業技術機密保護等經濟安全體制。

首先，日本財務省先後於 2017、2019 年修改《外匯及外國貿易法》，針對有危害國家安全之虞的外國投資設置嚴格審查基準。依據修法新規定，外資要投資擁有軍民兩用技術的日本企業或關鍵基礎事業，必須事前申報的出資比率由 10% 調降為 1%。同時，財務省據此制定執行辦法時，將核能、太空、網路安全等 12 項涉及國家安全的敏感技術產業指定為「核心產業」，規定外資必須事先經過審查才能持有 1% 以上股權，以嚴防外國透過對日投資、併購等途徑取得技術。

拜登於 2022 年 8 月 9 日，簽署重振美國半導體產業的《2022 年晶片和科技法案》，此法案將投入數百億美元的新資金，以促進美國半導體的研究和製造。（Photo Credit: The White House, photo by Erin Scott）

財務省
Ministry of Finance, JAPAN
国の信用を守り、
希望ある社会を次世代に引き継ぐ。

Google 提供 検索

English | 財務省FAQ | サイトマップ

財務省の政策 | 財務省について | 広報・報道 | 統計 | 申請・お問合せ

トップページ > 財務省の政策 > 国際政策 > 外為法関係・為替政策 > 外国為替及び外国貿易法（外為法）の概要 > 最近の外為法改正

最近の外為法改正

いいね！0　ポスト

● 2017年（平成29年）改正

1．改正の目的

安全保障の観点から、国の安全に関する投資に関し、無届け等で対内直接投資等を行った外国投資家に株式売却等の命令を行うことができる制度を創設したほか、外国投資家による他の外国投資家から非上場株式を取得する行為を審査付事前届出制の対象とする等、対内直接投資等規制の強化を行いました。

2．改正の概要

（1）特定取得の事前届出制対象への追加

国の安全を損なうおそれが大きい業種について、外国投資家による他の外国投資家からの非上場株式の取得を事前届出制の対象に追加しました。

（2）事後措置命令の導入

無届けや虚偽届出により対内直接投資等を行った外国投資家等に対し、国の安全を損なうおそれがある場合には、株式売却等の措置命令を行うことができる制度を導入しました。

● 2019年（令和元年）改正

1．改正の目的

日本経済の健全な発展に寄与する対内直接投資を一層促進するとともに、国の安全等を損なうおそれがある投資に適切に対応していくことを目的とし、事前届出免除制度を導入し、事前届出の対象を見直す等の改正を行いました。
（2020年５月８日施行）

2．改正の概要

（1）取得時事前届出免除制度の導入

一定の基準の遵守を前提に株式取得時の事前届出を免除する制度を導入しました。

（2）事前届出の対象の見直し

上場会社の取得時事前届出の閾値を10%から１%に引き下げたほか、役員への就任及び指定業種に属する事業の譲渡・廃止について、行為時事前届出を導入しました。

（3）国内外の行政機関との情報連携の強化

為防止重要技術及機密情報外流，日本政府嚴格控管外資對日企業之投資，日本財務省先後於 2017、2019 年修改《外匯及外國貿易法》，針對有危害國家安全之虞的外國投資設置嚴格審查基準。（資料來源：截自日本財務省，https://www.mof.go.jp/policy/international_policy/gaitame_kawase/gaitame/recent_revised/index.html）

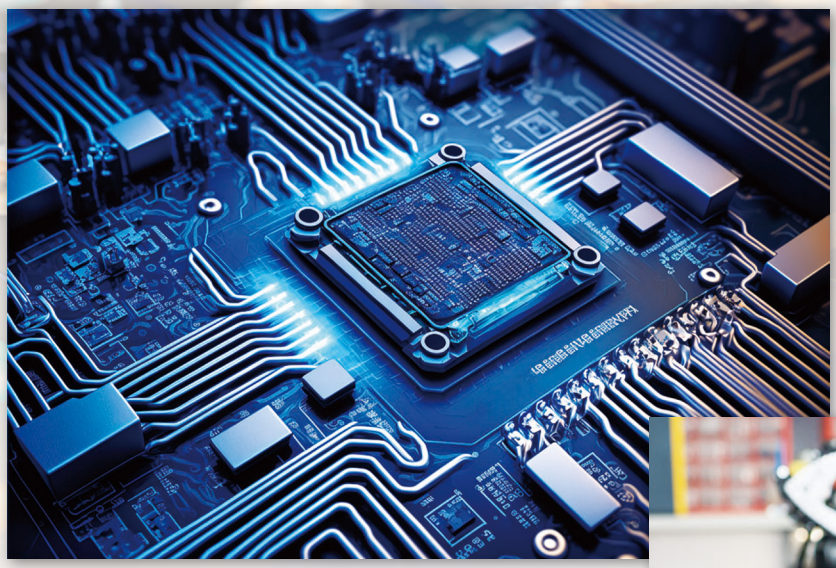
其次，經濟產業省、財務省、外務省等機關也分別設置經濟安全單位，而法務省公安調查廳也增加反情報工作的人員編制與預算，以因應外國產業間諜的威脅。2020 年 4 月 1 日，隸屬內閣官房的國家安全保障局新編制「經濟班」，負責彙整各省廳蒐報的經濟安全情報，提報內閣作為決策參考。2022 年 8 月 1 日，內閣府新設置「經濟安全擔當」大臣，並新編制「經濟安全保障推進室」，與國家安全保障局經濟班共同扮演確保日本經濟安全的指揮機制。

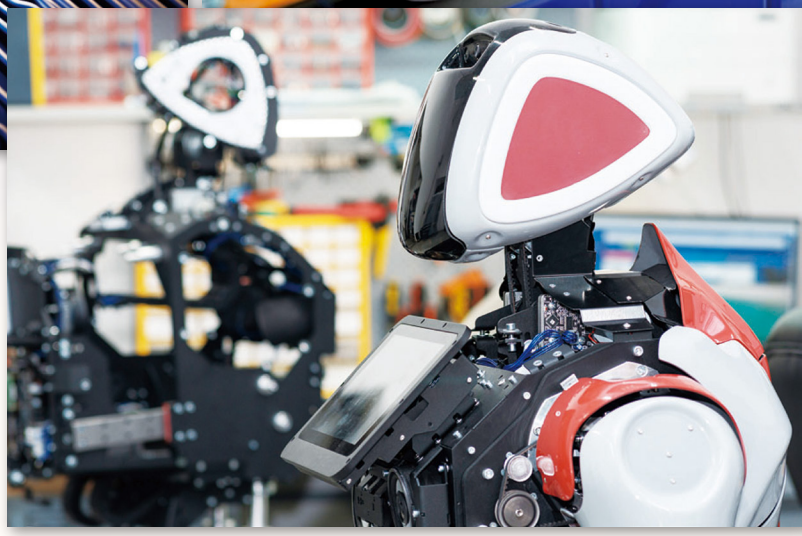
制定《經濟安全保障推進法》

為強化日本經濟安全，自民黨政務調查會「新國際秩序創造戰略本部」先後於 2020 年 12 月、2021 年 5 月向內閣提出政策建言，要求強化關鍵基礎事業的強韌性，以確保日本產業的「戰略自律性」，同時擴充、增強日本產業在國際社會的「戰略不可或缺性」。「戰略自律性」是要找出並克服日本重要產業鏈依存外國的瓶頸，「戰略不可或缺性」則是要發掘有助於日本企業發展新高科技並確保優勢，二者乃是日本經濟安全戰略的核心概念。

2021 年 11 月，日本首相岸田文雄在內閣設置「經濟安全保障法制準備室」，以及邀集專家學者組成「經濟安全保障法制有識者會議」，檢討建構確保日本經濟

2020 年 4 月，日本國家安全保障局新編制「經濟班」；2021 年 11 月日本內閣設置「經濟安全保障法制準備室」，並召開「經濟安全保障法制有識者會議」，檢討建構日本經濟安全的法體制。（圖片來源：日本首相官邸，https://www.kantei.go.jp/jp/101_kishida/actions/202111/19kanban.html）





安全的法體制。翌年 5 月 11 日，《經濟安全保障推進法》完成立法，其核心條文第二～五章依序揭櫫「確保特定重要物資的穩定供應」、「確保關鍵基礎設施的穩定使用」、「支援特定重要技術的開發」、「專利申請不公開」等 4 項制度。

該法的立法宗旨，主要在於保護關係到國計民生與國家安全的高科技產業、關鍵基礎設施、技術和資訊免受外敵危害，以及支援日本企業投入「特定重要技術」的研發。其後，岸田內閣依據該法，將半導體、蓄電池、機器人、重要礦物等共 12 項領域指定為「特定重要物質」。其次，再分批指定「特定重要技術」領域，迄今有海洋、太空航空、網路空間、遺傳以及跨領域等共 50 項技術被納入，並且設置 5 千億日圓「經濟安全基金」，以支援企業投入該等科技的研發。

同盟友邦合作確保經濟安全

另一方面，日本利用拜登政府重視同盟合作對應中共科技戰的機會，透過日美同盟、以及「四方安全對話」（Quadrilateral Security Dialogue, QUAD）、「七大工業國高峰會議」（Group of Seven, G7）、「印太經濟架構」（Indo-Pacific Economic Framework for Prosperity, IPEF）等多邊架構強化經濟安全措施。在日美同盟方面，日相菅義偉與拜登於 2021 年 4 月在美國白宮舉行會談，決定建構置焦於半導體、AI、量子技術、太空、資通等新高科技領域競爭力之「日美競爭力和韌性夥伴關係」，作為今後兩國合作強化供應鏈韌性的指針。翌年 1 月 21 日，日相岸田與拜登則是透過視訊會議，決定新設置由日本外務大臣與經濟產業大臣，以及美國國務卿與商務部長等四人組成的「日美經濟政策協議委員會」（經濟版「2+2」會議）架構，

岸田內閣依據《經濟安全保障推進法》，將半導體、蓄電池、機器人、重要礦物等共 12 項領域指定為「特定重要物質」。

商討如何強化供應鏈韌性以及「特定重要技術」之研發與保護。

其次，2021 年 3 月 12 日，由拜登主導舉行的 QUAD 視訊峰會，決定成立「新興關鍵技術工作小組」。2022 年 5 月 24 日，由日本主辦在東京召開的 QUAD 實體峰會，則發表「關於重要技術供應鏈原則共同聲明」，揭櫫安全性、透明性、自律性、健全性所構成的重要技術供應鏈原則，作為建構安全、有韌性、多樣化、持續可能的技術供應鏈之指針。此外，G7 輪值主辦國日本於 2023 年 5 月 22 日，在廣島召開 G7 峰會時，也將經濟安全設定為重要議題之一，並發表 G7 將合作強化供應鏈與關鍵基礎設施、強化對應經濟脅迫、新

QUAD 實體峰會是美國、日本、印度和澳洲之間的戰略對話，並以實現「自由且開放的印度太平洋」為目標。（圖片來源：日本首相官邸，https://www.kantei.go.jp/jp/101_kishida/actions/202205/24quad.html）

高科技之適切管理等措施的共同聲明。一周後，由美國主導在底特律召開、14 國加盟的 IPEF 部長會議也達成共識，決定建構供應鏈「危機反應網絡」早期警告機制，以確保供應鏈安全。

結語

美國對中共發動科技戰，凸顯確保供應鏈不斷鏈、新高技術不外流的經濟安全措施之重要性。由於該等措施並非美國單打獨鬥即可奏效的全球性議題，在拜登政府主導下，聯合同盟友邦共同對抗中共的經濟脅迫與科技霸權野心，因而讓日本經濟安全戰略與美國對中科技戰相結合，不但有助於強化日美同盟關係，也成功建構起 QUAD、G7、IPEF 等多邊架構，共同確保戰略性物資、新高科技關鍵零組件、醫療用品等供應無虞，以及新高科技不外流的經濟安全戰略部署。

兩強之間難為小？
試看蒙庫特與朱拉隆功的借鑑

◆ 世新大學兼任助理教授 — 宋啓成

良善的兩岸關係有益我國持衡發展，面對當前的緊張情勢，欲開創新局，19 世紀暹羅的經驗或許值得我們借鏡。

強權劍指之地

臺灣位處東亞花綵列島中心，戰略地位相當重要。1949 年底，中華民國政府播遷來臺，與大陸的中共政權隔海對峙；次年韓戰爆發，臺灣成為美國在東亞防堵共產勢力擴張之戰略布局一員，當時兩岸關係既緊張且嚴峻，並多次爆發戰事。

1970 年代起，美國與中共關係解凍，臺海情勢亦逐漸趨緩。1987 年臺灣開放赴大陸探親，兩岸交流日漸熱絡，更擴及觀光、產業、教育、文化、經濟等範疇。然中共企圖以武力解決兩岸分治的決心依舊未變，近年藉各種理由遏阻已行之有年的交流，並頻頻以機艦侵擾臺灣、發動軍演，

1950 年韓戰爆發，美國派遣部隊支援南韓，以對抗南進的朝鮮人民軍。

1987 年臺灣開放赴大陸探親，開放後 6 個月內湧現大量赴陸探親人潮，爾後兩岸交流日漸熱絡，更擴及觀光、產業、教育、文化、經濟等範疇。（圖片來源：國家發展委員會檔案管理局，https://www.archives.gov.tw/ALohas/ALohasColumn.aspx?c=2081）

而中共在南海、東太平洋海域的頻繁軍事活動，也引起周邊國家不安。

臺灣既是中共劍指所在，其戰略地位也是作為維繫東亞穩定要角的美國所不能忽視者。然臺灣處在美「中」兩強之間，一邊是攸關安全與生存的重要夥伴，一邊是有相同歷史淵源且互有往來的同文同種，任何一方皆難以割捨，也不願兵戎相見。面對當前局勢，臺灣究竟該如何因應？或許百餘年前的暹羅（即現今泰國）史實，可作為借鏡。

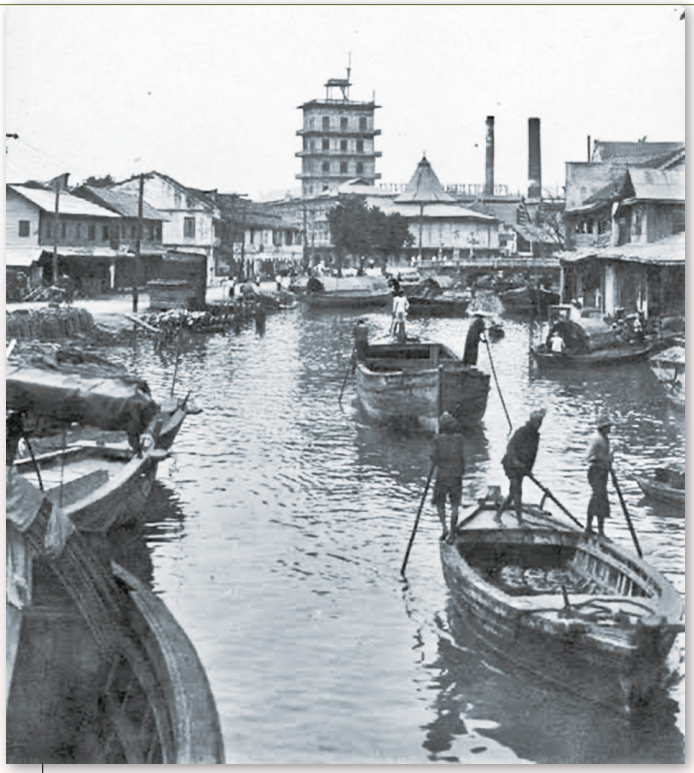
暹羅的靈活外交與現代化改革

19 世紀後期，整個東南亞幾乎淪為英、法、美、荷、葡等國的殖民地，只有暹羅仍維持獨立國家身分。當時，英國以印度為基礎，往東向緬甸及馬來半島、北婆羅洲擴張；法國自控制越南後，亦開始往西發展。這時的暹羅恰夾在英法擴張軸線之間，與臺灣所處的美中對峙態勢些許雷同。儘管英法兩國當時有把暹羅視為「緩衝國」（Buffer State），避免共處一道疆界的意圖；但此意圖最終能具體實現，應歸功暹羅國王拉瑪四世蒙庫特（Mongkut）與拉瑪五世朱拉隆功（Chulalongkorn）的靈活外交與現代化改革。[1]

1851 年登基的蒙庫特，目睹清朝敗於鴉片戰爭之慘狀，雖認清英國軍力強大之事實，但也希望守住固有傳統，不使列強有干預內政的藉口。遂一面大規模進行改革，派出代表團遠赴歐美，收集科學、交

[1] 薩德賽（D. R. SarDesai）著，蔡百銓譯，《東南亞史》，麥田文化，2001 年，頁 217。

拉瑪四世蒙庫特（左）與拉瑪五世朱拉隆功（右）對暹羅政治及社會施行現代化改革，成功避免暹羅成為西方國家的殖民地。



為鞏固國防與建設曼谷，拉瑪四世蒙庫特於 1851 年下令興建帕東功甲森運河（Khlong Phadung Krung Kasem），把整個曼谷城的範圍向外擴張了一倍。

通與政治制度資訊、敦聘顧問與工程師、翻譯西書、統合稅收、對各省及藩屬國訂定治理規則，且鼓勵人民向國王申訴司法案件；並為鞏固國防與建設曼谷，他下令興建一條 5 公里長的運河，每隔 1.5 公里設置沿岸砲臺，將此作法擴及到湄南河沿岸。[2] 另方面則從改變朝廷禮儀做起，豁免外國人四肢趴地匍伏接近國王「尊足」的慣例，也要求王子們學習英文，拓展國際觀，並允許外國人居住、通商及傳教。[3]

但這些作為並不足以抵擋列強的龐大勢力影響，必要時仍不免選擇讓步。由於有英法彼此存在矛盾，反倒給暹羅施展靈活外交的空間。當時清末遭逢的最惠國待遇、治外法權與關稅控制同樣出現在泰國，對任一國的讓步同樣須自動賦予其他簽約國。蒙庫特除藉以防範任何國家有取得最高優勢的機會，也在英法兩強之間分清比重。

當時的英國較法國強大，對貿易的興趣大過兼併領土；法國來勢洶洶，意圖打破柬埔寨是暹羅藩屬國的格局，強迫柬埔寨由法暹共管，擴大對柬國的影響力。對此，蒙庫特瞭然於胸，他決定給予英國更多利基，以爭取英國支持：英國在開採錫礦、原木及航運等方面擁有優勢，赴英留學的暹羅學生也比到其他國家為多，出身英國留學生的暹羅官員亦居多數。[4]

儘管有英國在暗中指導、協助，暹羅仍須獨自面對來自法國的威脅。1867

[2] 陳鴻瑜，《泰國史》，台灣商務印書館，2014 年，頁 202、205。
[3] 薩德賽，《東南亞史》，麥田文化，2001 年，頁 219。
[4] 薩德賽，《東南亞史》，麥田文化，2001 年，頁 220-222。

儘管有英國在暗中指導、協助，暹羅仍須獨自面對來自法國的威脅；圖為當時英國雜誌對法暹關係繪製的諷刺畫，飢餓的法國狼威脅地俯視湄公河對岸溫順的暹羅羔羊。（Photo Credit: Punch Magazine）

年 7 月，暹羅與法國簽署條約，柬埔寨成為保有獨立地位的法國保護國，未併入法國的交趾支那殖民地，暹羅則取得吳哥與馬德望省兩地。[5] 暹羅雖在柬埔寨問題對法國讓步，卻也給剛繼位的朱拉隆功國王持續改革與現代化的空間。為落實以暹羅作為緩衝的意圖，英法兩國於 1896 年共同發表協議，保證湄南盆地（Menam Basin）的統一與中立，兩國放棄在此區爭取絕對優勢，未獲對方同意不得派遣武裝部隊進入。這不僅保障暹羅的獨立，也改善了法暹關係。[6] 分清比重的靈活外交政策不僅保住暹羅，也得以持續發展。

上述暹羅與英法兩國間的態勢，有如國際關係學者摩根索（Hans J. Morgenthau）均勢理論（The blance of power）的競爭模式概念（如圖 1 所示）：當中的 C 國處在 A 國與 B 國之間，唯有 A、B 兩國力量處在均勢狀態，C 國的存在較易維持；若 A、B 兩國力量失衡，對 C 國反而影響更鉅。[7] 英國雖對暹羅提供幫助，但無意與法國開戰，暹羅對英國「一邊倒」絕非良策，需適度與法國保持友好，趁機強化自身，以面對更艱困的挑戰。

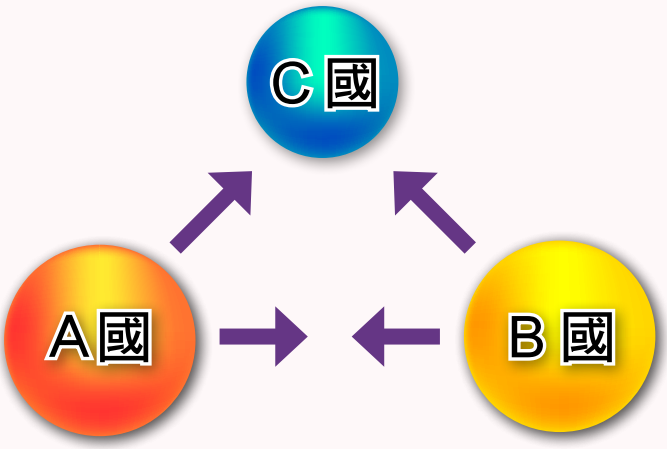


圖 1　摩根索均勢理論中的競爭模式

[5] 陳鴻瑜，《泰國史》，台灣商務印書館，2014 年，頁 206-207。

[6] 薩德賽，《東南亞史》，麥田文化，2001 年，頁 225-226。

[7] 摩根索（H. J. Morgenthau）著，湯普森（K. W. Thompson）改寫，孫芳、李暉譯，《國家間政治》，海南出版社，2008 年，第 6 版，頁 210-211。

2023 年 7 月至 9 月，中國北方及華南地區受颱風帶來的暴雨影響，發生多次嚴重水災，造成重大的人員傷亡與經濟損失。（圖片來源：中新社，https://w.wiki/9kkC）

強化自我實力　遏制強權侵擾

眼前臺灣與當年暹羅處在兩強對立間的處境類似，美國無意為臺灣輕啟戰端，中共來勢洶洶卻又投鼠忌器。多年來臺灣既得以持續存在，也爭取到寶貴時間強化自我，成為舉世讚譽的現代化與民主化典範。然而，面對兩岸軍力向中共傾斜，俄烏及以巴戰火使美國備多力分，在維持存在、自主的大前提下，暹羅的作法或許值得效法。

當時的法國除致力洗刷普法戰敗恥辱，還因英國占領埃及與擴大西非勢力範圍、展開海軍軍備競賽而關係緊張；[8] 如今中共雖受 COVID-19 疫情、洪澇災情等影響，內部政經問題也已焦頭爛額，然其國防預算依舊年年成長，且持續研製及採購新式裝備，推動國防及軍隊現代化。[9] 臺灣與泰國雖時地不同，但處境相似，面臨的都是戰爭威脅。倘若我國能效法當年的暹羅，擇選合適的兩岸議題主動遞出橄欖枝，藉以緩和兩岸緊張，爭取時間強化自我，從中營造有利態勢，或許是兩岸新局開創之際，值得思索的方向！

[8] 保羅 · 甘迺迪（Paul Kennedy）著，張春柏等譯，《霸權興衰史：1500 至 2000 年的經濟變遷與軍事衝突》，五南圖書出版，1995 年，頁 283-284。

[9] 中華民國 110 年國防報告書編纂委員會編，《中華民國 110 年國防報告書》，國防部，2021 年，頁 37；防衛省編，《令和 5 年版 日本の防衛—防衛白書》，2023 年，頁 56。

從證券交易管理機制初論「協同造假行為」的影響與應對

◆ 調查局認知戰研究中心 — 藍啟源

「協同造假行為」屬於境外敵對勢力操縱「灰色地帶」衝突及認知戰的具體手法，侵擾我輿論場域甚深。本文從市場機制及失靈角度出發，探討證券交易市場對詐欺和操縱行為的管理作為，類比意見市場中「協同造假行為」的查處，嘗試借鑒不同領域的經驗，提供應對之道。

為免市場機制失靈，政府宜適時介入

英國經濟學家亞當 · 斯密認為，市場中的參與者通過市場所反映的訊號提供行為準據，透過「看不見的手」（Invisible Hand）使資源的供需達成最適分配。然而他也強調市場機制並非無所不能，有時會面臨困境，此時就有政府介入必要；市場失靈（Market Failure）是其中一種典型原因。當市場無法有效提供價格信號給消費者和生產者，導致市場無法正常達成資源最佳配置，也無法實現社會所期望的目標，政府此時即應適當使用政策工具、立法管制介入。[1]

為免證券交易市場失靈，政府禁止市場詐欺及操縱行為

證券市場是企業向大眾募集資金的重要管道，也是國民經濟與投資的重要基石。

[1] 陳寶瑞，《公共經濟學》，五南圖書出版，100 年 1 月，二版，頁 3。

英國經濟學家亞當 · 斯密認為，當社會上的每個人都在追求私利時，市場就如同被「一隻看不見的手」所指引，資源的供給和需求將會自然而然達到均衡。

市場操縱是指有人蓄意干擾市場的自由和公平運行，最常見的就是證券操縱以及商品價格操縱，大多數國家都有立法禁止。

市場詐欺理論（Fraud-on-the-market Theory），闡釋證券市場參與者如果散布重大不實資訊，將嚴重影響市場，因為會使投資大眾基於錯誤的資訊進行交易，不僅是欺騙個別投資者，更是等同於對整體市場的詐欺行為。

市場操縱（Market Manipulation）行為，則包括故意創造供給、需求和價格、數量變動的假象，從而扭曲市場的自然運作。例如刻意以高價連續買進特定公司股票；或是連續以近似價位進行交易或委託。

前開兩種操縱市場行為，都會損害證券行情與市場公平和健全。因為其背後多是意圖營造股市熱絡或高漲假象，騙取散戶高價買入實質上不當值的股票，進而牟取利差的炒作集團。我國《證券交易法》，對前面提及的兩種行為都設有明確禁止的規範。該法第 155 條明確禁止操縱行為，而第 20 條則規範詐欺行為。

從意見市場理論角度出發，言論發表也是一種市場概念

意見市場理論概念，可追溯至 20 世紀初，由美國最高法院大法官奧利弗 · 溫德爾 · 霍姆斯提出，認為意見在發表前僅是對公共事務的看法或態度。但透過發表，意見就猶如商品一般投入市場自由交易，經由公開競爭和辯論，便能促使真相浮出水面；[2] 然而該理論對意見市場是否存有失靈情況，並沒有明確討論，但參照證券交易市場經驗，或可推論當意見市場被虛假資訊或操縱行為扭曲時，真相即可能被誤導，或被虛假觀點淹沒。

臺灣當前意見市場遭受「協同造假行為」嚴重侵擾

瑞典哥德堡大學的 V-Dem（Varieties of Democracy）計劃報告揭示，臺灣受到外國政府或其代理人假資訊攻擊的程度居

[2] 沃草烙哲學，〈失靈的意見市場：假消息、言論自由與真理理論〉，《沃草》，111 年 3 月 31 日，https://watchout.tw/forum/Oo0InB761rYf0YTxwohA。

調查局於 112 年 12 月發現臉書「不打烊便利店」粉絲專頁、「吳〇瑩」等帳號頁面發布深偽 AI 手法製作之影片搭配聳動標題，散布總統大選候選人有多名情婦之不實訊息，並利用我國社群常用圖文形式及習慣用語以假亂真。（圖片來源：法務部調查局，https://www.mjib.gov.tw/news/Details/1/953）

世界第一，[3] 反映臺灣意見市場遭受嚴重的侵擾。另由法務部調查局 111 年偵辦「茯苓兒有點甜」等粉絲專頁操弄 Covid-19 疫情訊息、[4]「兩岸頭條」等粉絲專頁傳播日本撤僑不實訊息、[5] 112 年查處「不打烊便利店」等粉絲專頁散布總統大選候選人情婦不實訊息 [6] 等案件新聞揭露資訊，也呈現相同的結果。由前開案件可發現，境外敵對勢力是透過社交平臺將此類造假資訊進行多層次轉傳散布，這樣的行為被稱為「協同造假行為」。

「協同造假行為」（Coordinated Inauthentic Behavior, CIB）概念是由 Meta 公司（FaceBook）所提出，[7] 指涉隱匿真實身分而透過社群平臺功能（社團、粉絲專頁等），以諸多帳號系統性地散布、炒作、傳散錯假訊息，[8] 從而扭曲公共討論的基礎，[9] 嚴重威脅民主體制運作。

[3] 菜市場政治學，〈台灣「接收境外假資訊」世界第一，調查怎麼做？〉，《鳴人堂》，108 年 4 月 12 日，https://opinion.udn.com/opinion/story/8949/3752204。

[4] 法務部調查局，〈境外敵對勢力認知作戰升級 國人宜謹慎識別網路假訊息〉，111 年 1 月 21 日，https://www.mjib.gov.tw/news/Details/1/756。

[5] 法務部調查局，〈調查局查獲中華〇〇公司收受大陸微視公司資金對臺進行認知作戰〉，111 年 11 月 18 日，https://www.mjib.gov.tw/news/Details/1/822。

[6] 法務部調查局，〈境外敵對勢力介入我總統大選 國人宜謹慎識別網路假訊息〉，112 年 12 月 20 日，https://www.mjib.gov.tw/news/Details/1/953。

[7] Nathaniel Gleicher, "Removing Coordinated Inauthentic Behavior," *Meta*, October 8, 2020, https://about.fb.com/news/2020/10/removing-coordinated-inauthentic-behavior-september-report.

[8] 胡元輝，〈境外資訊操弄是民主政治的敵人〉，《台灣事實查核中心》，108 年 8 月 26 日，https://tfc-taiwan.org.tw/articles/767。

[9] 時任臺北大學犯罪學研究所助理教授沈伯洋提出，「協同性造假行為」的假訊息通常由「內容農場」（content farm）生成，經過約半天即可將內容譯製成影片在不同社群頻道轉發，「每一個都可以得到 10 萬個點閱率」。此外，這些假訊息常會被放在「留言」處而不是發文處，因為這樣比較不容易被發現而導致帳號被禁刪，所以這些網軍會將假訊息貼在一般網路新聞的留言或評論。可參閱：鍾辰芳，〈專家：中國宣傳抗役、假信息多，特朗普反擊效果強〉，《美國之音》，109 年 3 月 21 日，https://www.voacantonese.com/a/experts-chinese-fake-news-on-coronavirus-hits-overseas-chinese-trump-push-back-beijing-narrative-20200320/5338825.html。

中共近年常對臺灣施加多樣化「灰色地帶」衝突威脅，包括戰機、艦繞臺之軍事手段，並透過虛假資訊投放、網絡攻防等手段，操弄輿論風向，動搖國人對政府政策的信心。（資料來源：國防部，中華民國 110 年國防報告書漫畫版，https://www.mnd.gov.tw/NewUpload/ 歷年國防報告書網頁專區 / 歷年國防報告書專區 .files/ 國防報告書 -110/110 年國防報告書 - 漫畫版 .pdf）

「協同造假行為」對社會的影響遠超一般錯誤資訊，因造假行為通常是有計畫、有系統且蓄意進行的，故更難以察覺；當虛假資訊充斥意見市場，公眾對重要議題的注意力和認知被誤導形成偏見，從而削弱公眾討論的建設性，並威脅社會共識的形成。

「協同造假行為」為「灰色地帶」威脅態樣「認知戰」的具體作為

境外敵對勢力近年對臺灣施加多樣化「灰色地帶」衝突威脅，包括戰機、艦繞臺之軍事手段，以及劃定貼近海峽中線之民航航線等非軍事手段，目的均在逐步升高威脅、消耗臺灣戰力及動搖民心，以改變兩岸現狀，達成「不戰奪臺」的目標。[10]

認知戰是「灰色地帶」衝突威脅的一種態樣，透過虛假資訊投放、網絡攻防等手段，企圖在平時藉著改變輿論風向來分化陣營；在戰時干擾政府及軍事指揮管制系統運作。[11] 對臺施加「協同造假行為」則是認知戰的具體操作手法。境外敵對勢力長期操作「協同造假行為」的結果，似已造成國人對政府政策的不信任感日益加深，公共議題的討論空間也因而受限。

[10] 中華民國 110 年國防報告書編纂委員會編，《中華民國 110 年國防報告書》，國防部，110 年，頁 41-44。

[11] 張玲玲，〈洞悉中共認知戰 鞏固全民心防〉，《青年日報》，110 年 6 月 18 日，https://www.ydn.com.tw/news/newsInsidePage?chapterID=1380128。

或可借鑒證券市場經驗，處理意見市場遭「協同造假行為」影響

正因「協同造假行為」對意見市場有著嚴重影響，但其行為模式也與證券交易市場中的市場詐欺及操縱行為極為雷同，兩者存在許多相似之處，故或可借鑒證券交易法的經驗，應用於意見市場以處理「協同造假行為」的影響。

在證券市場與意見市場中，資訊的真實性和透明度均是順利運作的基礎；詐欺和操縱行為扭曲證券市場資訊，導致投資者無法根據真實情況作出決策，也會破壞投資者對市場的信任；同理，「協同造假行為」同樣阻礙意見市場公眾對議題的真實理解，並損害其對資訊來源的信任。在這兩種情況下，公眾信任的喪失，都對市場的穩定性和有效性造成長期影響。

然而，由於涉及言論自由的保護，且意見市場參與者涵蓋個人、媒體、社群平臺業者、政府部門等，遠超過證券市場的參與者，建立針對意見市場詐欺與操縱行為的監管機制，顯得更為複雜和困難，非直接套用證券交易法令條文就可以解決。況且，「協同造假行為」偵測、用戶資訊調取及爭議訊息下架，更涉及各社交平臺業者配合意願，並非如同證券市場有金融監管機構配合，甚可主動產出可疑交易報告，因此在打擊「協同造假行為」和保護言論自由間找尋平衡點，顯得更加困難。

結論與展望

本文期望透過應用證券交易市場的相關理論，為理解和應對當前意見市場中日益嚴重的「協同造假行為」提供新的視角。儘管在運作機制和管理框架上存在差異，但兩種市場在維護資訊的真實性和透明度、保護公眾信任方面，有著相似的目標，並面臨相同的挑戰。同時，保護資訊的真實性，對於維護意見市場的健全與公共討論的品質至關重要，但在設計監管策略和機制過程中，主政者仍須謹慎考慮，在保護言論自由與避免過度干預之間，取得平衡。

意見市場參與者眾多，涵蓋個人、媒體、社群平臺業者、政府部門等，因此建立針對意見市場詐欺與操縱行為的監管機制非常複雜且困難，並非直接套用證券交易法令條文就可以解決。

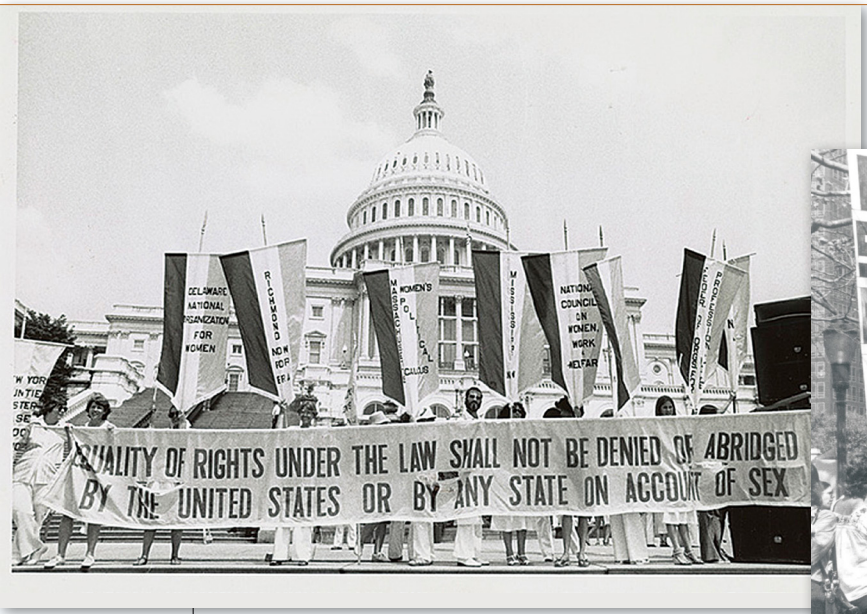
非自願獨身者運動之發展與進化

◆ 調查局國際事務處前專門委員 — 陳能鏡

非自願獨身者運動（Incel movement）是國內恐怖主義最新威脅，世界各國執法與反恐機關應認識其發展脈絡、特徵及所帶來的真正威脅，才能擬訂可行有效的對策。

仇女意識之萌芽

1960 年代興起新一波女權運動，專注於批判父權體制，爭取女性身體自主權，希望在社會及經濟上獲得全面性的平等，美國的女性主義者甚至於 1966 年創立全國婦女協會（National Organization of Women），採取行動與措施，協助女性在美國社會主流中，行使所有經此而與男性有實際同等夥伴關係的特權與責任。這一波的女權運動確實有快速而驚人的進展與成果，但也導致傳統父權體制的崩解，許多男性認為女性天生為男性提供愛情、性、生育等服務，但這些天賦的特權卻被女性主義者偷走或掠奪，他們才是真正受壓迫及被剝奪的一群，他們尋求解放，甚至想要奪回男權與優勢。職是之故，1970 年代興起反女性主義的男權運動，包括 1977 年成立的全國男性解放聯盟（National Coalition for Free Men）。



1960 年代興起一波女權運動，專注於批判父權體制，爭取女性身體自主權，希望在社會及經濟上獲得平等；圖為美國全國婦女協會於 1979 年為女權發聲的示威遊行運動。（Photo Credit: the WHITE HOUSE, photo by Bettye Lane, https://obamawhitehouse.archives.gov/blog/2015/06/30/day-history-national-organization-women-was-founded）

男性的焦慮與挫折轉變為敵意的厭女社會結構，建構起男性至上社群，例如：男權運動、男人自行之路、搭訕藝術家、父權團及非自願獨身者。（Photo Credit: TechComingSoon, https://w.wiki/9kGa）

當代的西方社會已不再承認男性的主導角色，致許多男性充滿迷失感、受壓迫感及挫折感，若再與女性主義導致男性優勢與霸權岌岌可危的男性氣概危機（crisis of masculinity）相連結，男性的焦慮與挫折轉變為敵意的厭女社會結構，男性氣概質變為「有毒男性氣概」（toxic masculinity），[1] 進而激進化為仇女情結（misogynistic complex）的次文化氛圍，建構起激進男性圈社群（nanosphere communities），或稱男性至上社群（male supremacy communities），例如：男權運動（Man's Rights Movement）、男人自行之路（Men going Their Own Way）、搭訕藝術家（Pick Up Artists）、父權團（Fathers' Rights Group）及非自願獨身者（Incel）。1989 年 12 月，加拿大發生蒙特婁理工學院（Montreal's Ecole Polytechnique） 槍擊案，不但是有紀錄可查的第一起仇女謀殺案，也一度是加國史上傷亡最慘重的槍擊案。[2]

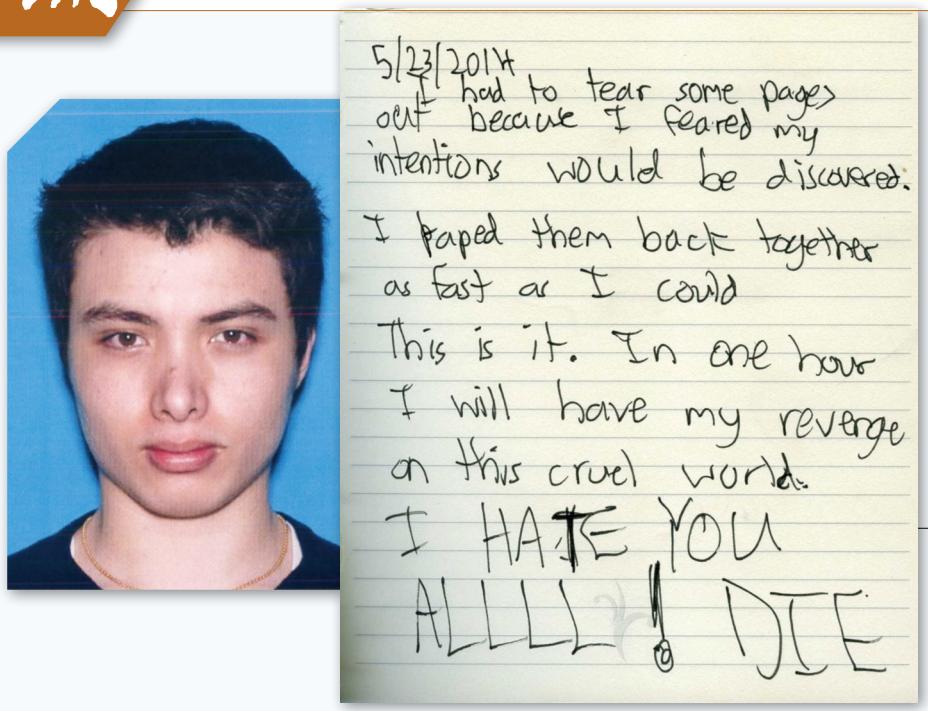
非自願獨身者運動之成形

一、線上獨立仇女運動

Incel 是 involuntary celibate 的合成字，他們是一群自認被女性拒絕而被迫無法發展情愛關係的孤獨男性，其中部分屬仇女非自願獨身者（misogynist incels），他們心中充滿仇恨與不滿，把自己的不幸

[1] 美國民權組織反誹謗聯盟（Anti-Defamation Leage）在其 2021 年度的「美國謀殺與激進主義」（Murder & Extremism in the United States）報告中，三大類右翼激進主義分別為：白人至上主義、反政府激進主義及非自願獨身者或男性圈激進主義（Incel/Manosphere Extremism），但在 2022 年及 2023 年度報告中，第三類改稱為「有毒男性氣概激進主義」（Toxic Masculinity Extremism），顯示仇女激進分子仍無普遍的專有名詞。本文仍沿用較常見之 Incels。

[2] 請參閱拙作〈性騷與仇女恐怖主義〉，《清流雙月刊》，2023 年，第 48 期，頁 50-56。



2014 年 5 月犯下美國加州伊斯拉維斯塔槍擊案的槍手羅傑（左圖），在非自願獨身者社群中被尊崇，為後續大規模槍擊案或仇女謀殺案罪犯讚揚、模仿的對象；右圖為羅傑犯案前滿懷憤恨的手寫日記。

歸責於女性，自認有權以暴力侵害他人。1990 年代，網路與線上論壇普及，加速仇女意識型態散播，也加深仇女意識的濃度與厚度。另一方面，男性至上社群勢力也發生重大變化，男權運動者與搭訕藝術家信徒日漸減少，轉投入男人自行之路與非自願獨身者，特別是後者，非自願獨身者社群成員大幅成長，也更仇女與狠毒。

2014 年 5 月美國加州發生伊斯拉維斯塔槍擊案（Isla Vista Shooting），此案不是男性至上主義者（male supremacist）犯下的第一起大規模槍擊案，但卻是往後一波仇女謀殺案的起點，也帶動仇女非自願獨身者社群的快速發展與擴散，更促成非自願獨身者結合成一種運動，而與其他的線上男性主義者社群分離，非自願獨身者運動正式成立。該案槍手羅傑（Elliot Rodger）在非自願獨身者社群中，被尊為「守護神」（patron saint）、「烈士」（martyr）、「真正的前輩」（true progenitor）等，作案日 5 月 23 日被尊列為「聖艾略特日」（St. Elliot Day）而加以慶祝，在往後的大規模槍擊案或仇女謀殺案中，不時被案犯提及，甚至讚揚或模仿。

二、三大特徵

男性至上主義研究所（Institute for Research on Male Supremacism）共同創辦人兼研究員凱莉（Megan Kelly）為文指出，[3] 女性獸化（dehumanization）、男性固有性權利（male sexual entitlement）及暴力崇尚是仇女非自願獨身者運動的三大特點，茲概述於後。

（一）女性獸化：各種型態的女性獸化是仇女非自願獨身者運動的核心理念，將女性形容成一群凶殘的動物，同時也必須以動物待之，女性獸化激發了輕蔑與憎惡的感覺，藉以支持大規模屠殺的合法性與光

[3] Megan Kelly, Alex DiBranco, & Dr. Julia R. DeCook, "Misogynist Incels and Male Supremacism, New America," 2021. 該報告共 37 頁，對仇女非自願獨身者運動的發展、特徵、論述等有非常詳細之敘述。

榮性。美國專研危險言論學者創建的「危險言論項目」（Dangerous Speech Project）研究發現，獸化是危險言論的品質保證，而危險言論為意識形態激進主義者為實施暴力而撤除禁令。

（二）**男性固有性權力**：男性固有性權力的核心是將獸化後的女性歸類次等，視女性是生而為服務男性的工具，認為提供男性性滿足與性享樂是女性的榮耀、金髮美女是一件可以交換或相互擁有的物品。

（三）**暴力崇尚**：非自願獨身者運動分子讚揚仇女大規模槍擊案主嫌，也讚揚沒有非自願獨身者背景的大規模槍擊案犯或重大爆炸案恐怖分子，如 2017 年拉斯維加斯大規模槍擊案（60 死、逾 500 傷）犯嫌，以及 1995 年奧克拉荷馬市聯邦大樓爆炸案（168 死、逾 680 傷）與 2007 年維吉尼亞理工大學槍擊案（32 死、23 傷）主嫌等。

三、仇女意識與種族歧視合流

非自願獨身者運動充滿種族歧視，許多非自願獨身者將其不受女性青睞原因，歸咎於他們的種族背景，自稱為「稻米非自願獨身者」（ricecels）或「咖哩非自願獨身者」（currycels），表明女性較鍾情於白種男性。事實上，這些標籤主要被白種非自願獨身者所使用，他們心中只有白人與非白人之分，非屬白色人種的非自願獨身者統稱「ethnicels」，蔑稱東南亞裔人為「ricecels」，南亞人為「currycels」，只有純白人才是天選的「白馬王子」，另在仇女非自願獨身者社群中，「JBW」（Just Be White）是非常常見的貼文，顯示白種

美國專研危險言論學者創建的「危險言論項目」研究發現，獸化是危險言論的品質保證。

非自願獨身者運動分子讚揚仇女大規模槍擊案主嫌，也讚揚沒有非自願獨身者背景的大規模槍擊案犯或重大爆炸案恐怖分子，如造成死傷慘重的 1995 年奧克拉荷馬市聯邦大樓爆炸案主嫌。（Photo Credit: FBI, https://www.fbi.gov/image-repository/okbomb.jpeg/view）

男性的種族優越感，也彰顯了白人至上主義信條對非自願獨身者運動的影響力。

在德國，仇女意識與極右思潮有著強烈的連結，且將種族議題混入非自願獨身者運動。2020 年 2 月，黑森邦哈瑙（Hanau）連續槍擊案中，43 歲犯嫌在其宣言中表明，他是位非自願獨身者，仇視移民也厭惡女性，因此受害人皆有移民背景，作案地點選在中東庫德族人常去之水煙館。[4]

最新恐怖主義威脅

2015 年 10 月美國安普瓜社區學院槍擊案（Umpqua Community College Shooting）犯嫌 Chris Harper Mercer、2017 年 12 月美國阿茲特克高中槍擊案（Aztec High School Shooting）犯嫌 William Atchison、2018 年 2 月美國帕克蘭高中槍擊案（Stoneman Douglas High school, Parkland）犯嫌 Nicolas Cruz、2018 年 4 月加拿大多倫多仇女謀殺案犯嫌 Alex Minassian、2018 年 11 月美國塔拉哈西熱瑜珈教室槍擊案（Tallahassee Hot Yoga Studio Shooting）犯嫌 Scott Beierle 等，均在其宣言或線上論壇中讚揚或多次提及羅傑，其中有人被確認為非自願獨身者運動的一員，有人被歸類為該運動的同情者，犯案動機可直接或間接連結到非自願獨身者運動之意識形態。

犯下 2018 年美國帕克蘭高中槍擊案的犯嫌 Nicolas Cruz 在其宣言或線上論壇中讚揚或多次提及羅傑，犯案動機可連結到非自願獨身者運動之意識形態。

至 2019 年底，美、加仇女槍擊案死亡人數近 50 人，非自願獨身者運動意識形態真實存在且致人於死；有鑑於此，美國喬治城大學安全研究學程教授霍夫曼（Bruce Hoffman）於 2020 年 1 月，以「非自願獨身者：美國最新國內恐怖主義威脅」（Incels: America's Newest Domestic Terrorism Threat）為題，[5] 呼籲執法及反恐機關應承認非自願獨身者運動所帶來真實且持續增加的威脅，理由有五：

1. 男性至上父權體制社會觀賦予壓制女性的當然權利
2. 線上激進化、動員及通訊快速擴大及增加知名度與關注度
3. 孤狼暴力行為挑戰執法人員事先防制與初期壓制的能力

[4] 凱莉認為，本案犯嫌雖在宣言中提及已有 18 個月未曾和女性發展關係，但不能證明他是一名懷有仇女意識型態的非自願獨身者，故本案非屬仇女恐攻案。

[5] 霍夫曼也是美國知名智庫外交關係協會（Council on Foreign Relations）反恐及國土安全資深研究員；另該文第二作者 Jacob Ware 為喬治城大學兼任教授。

4 非自願獨身者意識形態與極右激進主義相互混雜與激盪

5 無障礙可及性吸引性挫折男性陷入非自願獨身者的虛擬國度

美國知名智庫戰略及國際研究中心（Center for Strategic & International Studies, CSIS）跨國威脅計畫主任瓊斯博士（Seth G. Jones）同年亦在「美國持續升高的恐怖主義問題」一文指出，[6] 右翼激進主義是美國最嚴重且將持續威脅的恐怖主義，右翼恐怖分子及網絡可分三大類，即白人至上主義者、反政府激進分子及非自願獨身者，其有三項共通性：

1 均採分權模式運作，威脅來自個人而非網絡

2 採線上招募、組訓及遂行任務，徒增執法人員鎖定潛在目標困難度

3 與蓋達（al-Qaeda）、伊斯蘭國（ISIS）等國際恐怖組織相互學習及採用戰術

承認威脅才能有效防制

宗教恐怖主義有其神祕難懂的教義，政治激進主義有其複雜深奧的政治理論，此二類非經特定人士的闡釋與宣揚，非教中或圈內人不易領會及狂熱，支持者或信徒增加相對緩慢，擴張與外溢效果與速度受到限制；非自願獨身者運動雖歸類為右翼恐怖主義，但有高度社會性，世界各地年輕男性每天都可能經歷性挫折與孤獨情緒，只要幾個點選，即可進入暗黑非自願獨身者國度，不自覺中接受激進意識，快速成為潛在仇女恐怖分子。

由於網際網路的活躍，非自願獨身者可輕易透過線上發表激進言論，群聚於具有相同意識的虛擬世界中，藉此跨大非自願獨身者運動的規模與關注度。

研究顯示，性別越平等的民主社會，厭女的氛圍越是強烈，仇女恐怖主義犯罪的潛在危險越高；如同美、加與西歐英、德諸國，臺灣在追求兩性平權過程中，也出現反對聲浪與反噬現象，如「母豬母豬，夜裡哭哭」、「臺女就是賤」等汙辱與嫌惡女性的言論，某大學學生會性平委員會選舉，甚至出現「一拳一個自助餐」、[7]「制裁臺女」等暴力仇女政見，已將非自願獨身者運動的三大特徵，從虛擬世界搬到真實世界來主張與推動，此等社會扭曲現象，值得吾等關注與研究，要認識與承認其威脅，才能擬定對策及有效防制。

[6] Seth G. Jones, Catrina Doxsee, & Nicholas Harrington, “The Escalating Terrorism Problem in the United States,” June 17, 2020, Center for Strategic & International Studies.

[7] 指女性藉由平權論述，選取對自己有利部分，而不願承擔相對之義務，如同吃自助餐，只取用自己想吃的。

可程式邏輯控制器（PLC）之安全

◆ 華梵大學資管系特聘教授 — 朱惠中

2024 年的資安環境充滿了挑戰，幾乎每個行業的網路攻擊都在增加，並且在可見的將來沒有任何放緩的跡象。

以可程式邏輯控制器（Programmable Logic Controller, PLC）來說，上個世紀末期，網路犯罪分子主要的攻擊方法在致力於存取 PLC 的資訊及直接干擾特定程序，而現今則進入了更高的情報層次，駭客可以透過 PLC 來存取整個網路系統，從而加劇能夠製造的混亂。目前，我國關鍵基礎設施中有關水利、石油以及電力等領域的控制系統均已使用 PLC。

何謂可程式邏輯控制器（PLC）

PLC 是一種以數位動作之電子裝置，它使用可程式記憶體以儲存指令，執行像是邏輯、順序、計時、計數與演算等功能，並透過數位或類比輸入輸出模組，控制各種的機械或工作程式。

PLC 基本結構大致上包含中央處理單元、記憶體與輸入／輸出等單元（如圖 1），簡略說明如下：

一、中央處理單元（CPU）

用掃描的方式採集由現場輸入裝置送來的狀態或資料（電壓或電流等類比訊號），分析後再按指令規定的任務產生相應的控制信號，去指揮有關的控制電路。

二、記憶體（Memory）

記憶體主要用於存儲程式及資料，通常也可使用 RAM 或 EEPROM 等專用記憶體卡片方式擴充。

三、輸入／輸出單元

由 CPU 處理已書寫在 PLC 裡的程式指令，判斷驅動輸出單元，進而控制外部負載，如指示燈、電磁接觸器、繼電器、氣（油）壓閥等。

四、通訊網路模組

目前 PLC 大多具有可擴充通訊網路模組的功能，它使 PLC 與 PLC 之間、PLC 與個人電腦以及其他智慧型裝置之間能夠交換資訊。一般 PLC 通訊協定規格可分為 RS-232、RS-422、RS-432、RS-485、IEEE 1394、IEEE-488（GPIB）。目前國際中最常用的通訊協定包含：Modicon 公司所制定的 MODBUS-ASCII 模式及 MODBUS-RTU 模式、西門子公司所制定之 PROFIBUS 以及日本三菱電機所推出 CC-LINK 等通訊協定。

PLC 系統之外部裝置可區分成以下四大類：

一、編程裝置

有簡易編程器和智慧型圖形編程器，用於編程、對系統作一些設定、監控 PLC 及 PLC 控制系統的工作狀況。編程器是 PLC 開發應用、監測運行、檢查維護不可缺少的工具，但它不直接參與現場控制執行。

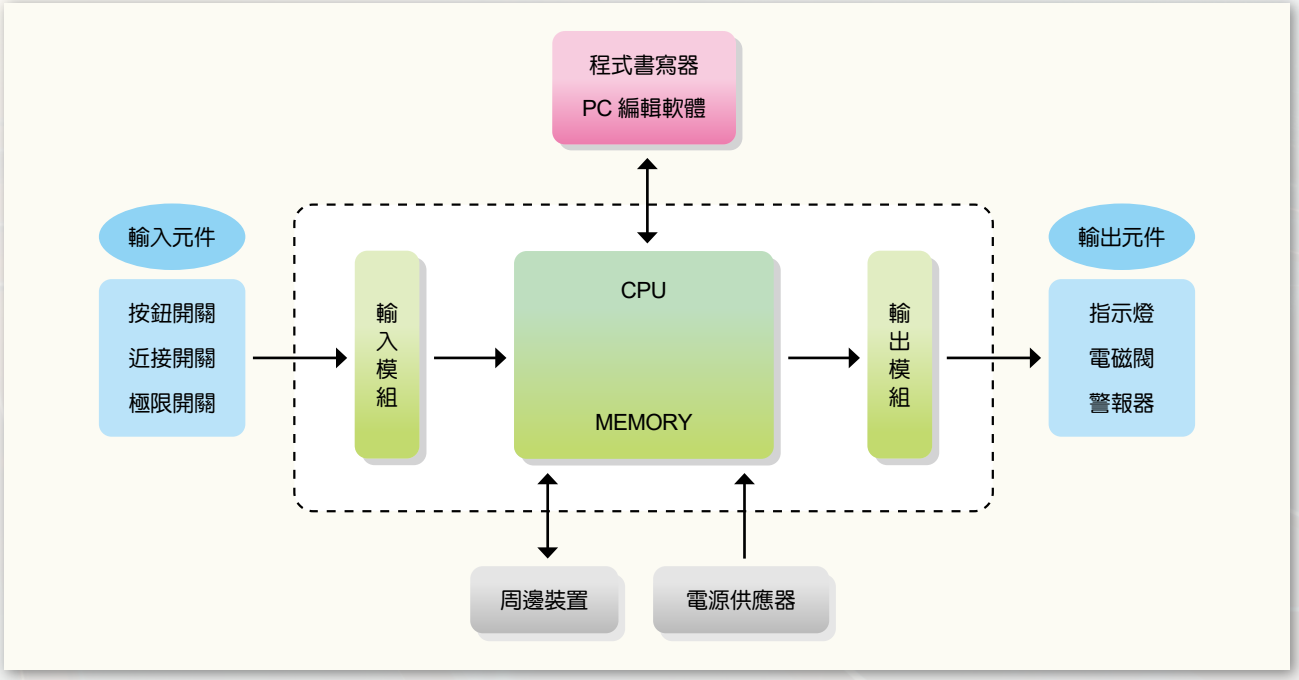
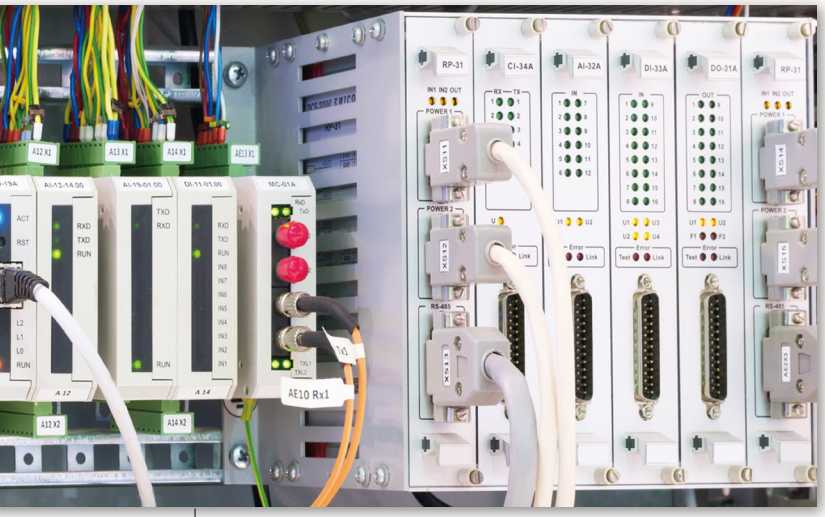
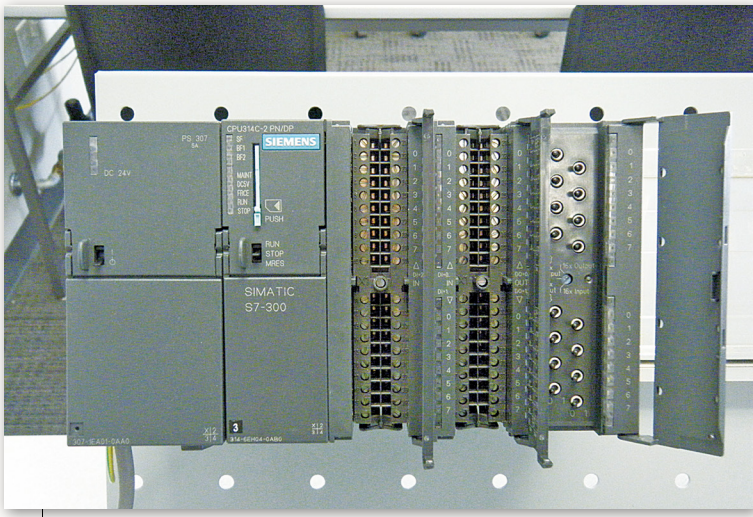


圖 1　PLC 基本結構圖



PLC 大多具有可擴充通訊網路模組的功能，它使 PLC 與 PLC 之間、PLC 與個人電腦以及其他智慧型裝置之間能夠交換資訊。



PLC 系統外部裝置可區分成編程裝置、監控裝置、存儲裝置、輸入輸出裝置四大類。（Photo Credit: Robert Kevin Moore, https://flic.kr/p/dYDqzb）

二、監控裝置

資料監視器和圖形監視器，例如直接監視資料。

三、存儲裝置

有存儲卡、存儲磁帶、軟碟或唯讀記憶體，用於永久性地存儲用戶資料。

四、輸入輸出裝置

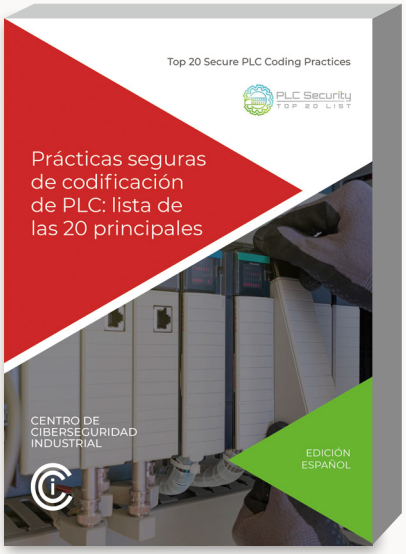
用於接收信號或輸出信號，一般有條碼讀入器、輸入模擬量的電位器、印表機。

PLC 的編程程式語言既要滿足易於編寫，又要滿足易於調試的要求。目前，還沒有一種對各廠商軟硬體產品都能相容的編程語言，1993 年 12 月，國際電工委員會（International Electrotechnical Commission, IEC）制定 IEC 61131-3 標準，用於規範 PLC 編程系統的標準，使得應用 IEC 61131-3 標準已經成為工業控制領域的趨勢。現今，PLC 編輯軟體只需符合 IEC 61131-3 國際標準規範，便可藉由符合各項標準的語言架構，進而建立任何人皆可瞭解的程式。此標準最終目的是讓 PLC 的使用者在不更改軟體設計的狀況下可以輕易更換硬體（HOT-SWAP）。*

設計、開發與撰寫安全的 PLC 程式的準則

凡是可程式設計（Context-Sensitive）的語言都有它的安全編碼規範，比如 PASCAL、C 等諸多電腦語言，鑒於工業控制系統也是一個可程式設計的系統，他們也應該擁有自己的安全編碼規範或者代碼風險管理措施。基於此，國際自動化學會（International Society of Automation, ISA）的網路安全小組（Network Security Group）於 2021 年 6 月 15 日發布《可程

* 摘自《關鍵資訊基礎設施防護參考指引》。



ISA 的網路安全小組於 2021 年發布《可程式邏輯控制器的 20 項主要準則》，避免工業控制系統運行過程中出現的各類錯誤，並為調查相關安全事件提供參考。（Source: admeritia GmbH, https://www.plc-security.com/index.html）

式邏輯控制器的 20 項主要準則》（Top 20 Secure PLC Coding Practices），目的是讓我們意識到，雖然安全編碼規範並不能完全阻止網路攻擊，但是它可以避免工業控制系統運行過程中出現的各類錯誤，並為調查相關安全事件提供一些參考。

《可程式邏輯控制器的 20 項主要準則》

1. PLC 程式碼模組化：使用不同的功能區塊（副程式，Subroutine），將 PLC 程式碼拆分為多個模組，並獨立測試每一副程式模組。

2. 追蹤運行模式：保持 PLC 處於執行（RUN）模式，如果 PLC 不處於 RUN 模式，應該通知操作人員。

3. 盡可能利用 PLC 來做運算邏輯（例如累加或積分），不宜過度依賴人機介面（HMI）來做。

4. 使用 PLC flags 作完整性檢查：在 PLC error flags 上放置計數器以捕獲任何數學問題，如改變其邏輯、啟動新程序、測試新代碼、下載新的程序等等，由於大多數的 PLC 不提供加密、完整性的檢查，如發生上述邏輯的更改，Flags 可以是很好的指示。

5. 使用加密及 Checksum 之完整性來檢查 PLC 代碼，使用加密雜湊或校驗和（如果加密雜湊不可用）來檢查 PLC 程式碼完整性並在程式碼發生變更時發出警訊。

6. 驗證定時器和計數器：如果定時器和計數器值會寫入 PLC 程序中，為了符合合理性（定時器或計數器預設的有效範圍及歸零）之要求，PLC 須先驗證寫入值的合理性，並且需驗證輸入值小於零時計數器反向計數情況。

7. 配對輸入／輸出的驗證和警訊：如果您有成對訊號，請確保兩個訊號不會同時有相同的值，當發生物理上不可能的輸入／輸出狀態時（如輸入與輸出均是「ON」），請立即通報操作員；為防止切換輸出可能損壞執行器（Actuator），可考慮使成對訊號獨立或新增延遲計時器。

8. 在 PLC 層級上須先驗證 HMI 輸入之變數值，並應在 PLC 中增加進一步的交叉檢查，以防止或警告超出可接受範圍的值編程到 HMI 中。

9. 驗證間接用來驗證 PLC 變數的完整性：通過對陣列的溢出或異常下標輸入來驗

證間接指令，以捕捉「柵欄柱（fence-post）錯誤」；因 PLC 通常沒有「陣列結束」標誌，因此最好在軟體中建立它，其目標是避免異常或計劃外的 PLC 操作，亦即設定陣列的範圍。

10. 依特定功能分配指定暫存器區塊（讀／寫／驗證），以驗證資料、避免緩衝區溢位並阻止未經授權的外部寫入以保護控制器資料。

11. 合理性檢查工具：允許透過交叉檢查不同測量值來進行合理性檢查，並對過程進行儀表化。

12. 根據實體合理性驗證輸入：確保只能輸入流程中實際或物理上可行的內容；操作設定計時器，使其達到實際所需的持續時間；當出現偏差時考慮發出警報，另當出現意外的不活動時，也應提醒操作員。

13. 停用不需要或未使用的通訊埠和協議：PLC 控制器和網路介面模組通常支援多種預設啟用的通訊協議，停用應用程式不需要或未使用的連接埠和協定。

14. 限制第三方介面的連接類型和可用資料：連接資料介面應明確定義並限制為僅允許所需資料傳輸的讀取／寫入功能。

15. 定義 PLC 重新啟動時製程的安全流程狀態（例如，為觸點通電、斷電、維持先前狀態）。

16. 每 2-3 秒總結一次 PLC 循環時間並傳送給 HMI 以在圖表上進行視覺化處理。

17. 記錄 PLC 正常運作時間並在 HMI 上執行趨勢分析，以利進行診斷。

18. 記錄因故障或急／硬停機而造成 PLC 停機事件，以便 HMI 警報系統檢索，可在 PLC 重新啟動之前查詢更精準的時間資料，並在 HMI 上繪製趨勢圖。

19. 監控 PLC 記憶體使用量，並提供生產環境中部署的每個控制器的記憶體使用基準，以利在 HMI 上進行趨勢分析。

20. 關鍵警訊的誤報和誤判：當 PLC 發現關鍵警訊為誤報和誤判時，應記錄造成此誤報和誤判的資訊，並阻止此關鍵警訊誤報和誤判繼續發生。

PLC 被攻擊的案例

PLC 之安全在日常生活中對關鍵基礎設施的影響性甚大，詳述如下。

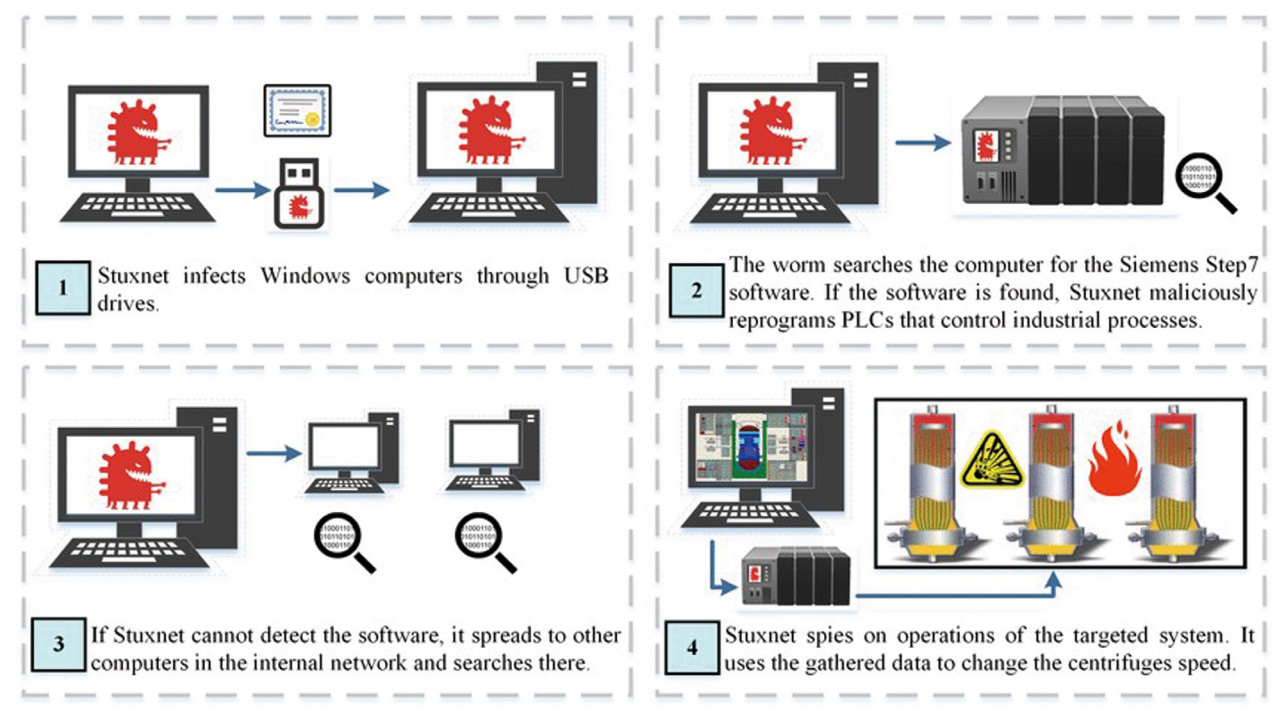
一、能源

1. 震網（Stuxnet）事件

駭客利用西門子公司控制系統（SIMATIC WinCC/Step7）存在的漏洞，向 PLC 寫入代碼並將代碼隱藏。這次事件是有史以來第一個包含 PLC Rootkit 的電腦蠕蟲，也是已知的第一個以關鍵工業基礎設施為目標的蠕蟲。據報導，該蠕蟲病毒可能已感染並破壞了伊朗納坦茲的核設施，並最終使伊朗的布希爾核電站延遲啟動。

2. 停電

北美遭駭客利用 PLC 中的漏洞對關鍵基礎設施和工業環境造成破壞，該兩個漏



震網事件是已知第一個以關鍵工業基礎設施為目標的蠕蟲，該病毒可能已感染並破壞了伊朗納坦茲的核設施，並最終使伊朗的布希爾核電站延遲啟動。（Photo Credit: Charalambos Konstantinou, https://www.researchgate.net/publication/340331302_Security_Analysis_of_Smart_Grid）

洞都位於物理控制操作技術設備的 PLC 通訊模組中，並能透過惡意的通用工業協定訊息（Control and Information Protocol, CIP）觸發，能修改流經 PLC 之數據及觸發拒絕服務（DoS），導致裝置無法操作，此次除造成該縣大停電外，相關能源與交通運輸亦受到影響。

3. 水資源

澳洲昆士蘭省黃金海岸的馬盧奇郡（Maroochy Shire），其新建的污水處理系統之工業控制系統被前任承包商員工利用筆記型電腦與無線電發射器控制 142 個 PLC（包括污水抽水站、2 個監控站與 3 個無線電頻道），3 個月內造成 46 次、超過 26 萬 4,000 加侖的污水進入地區供水系統。

二、以色列 Unitronics PLC 遭伊朗攻擊利用

據安碁公司 2023 年 11 月「威脅情資研究中心 OT 威脅觀察與分析」月刊報導，伊朗政府伊斯蘭革命衛隊（IRGC）附屬的 APT 組織，針對包括美國 WWS、能源、食品和飲料製造以及醫療保健等多個領域利用 Unitronics 可程式邏輯控制器進行攻擊活動；攻擊者利用 HMI 破壞了 Unitronics Vision 系列 PLC，將這些受感染的裝置使用預設密碼公開在網路上。

駭客攻擊關鍵基礎設施：低調、緩慢且毀滅性十足

阻止網路攻擊並不是某一個環節、一個設備就能完成的，它需要從工控系統本體、安全編碼、外部防護設備、軟體系統、管理運維、緊急應變計劃與回應等多個體系或者維度一起努力才能達到，PLC 是構建工業控制系統安全防護體系必不可少的一個環節。

國家關鍵基礎設施軟體供應鏈安全初探

◆ 國防大學兼任助理教授 — 張喻閔

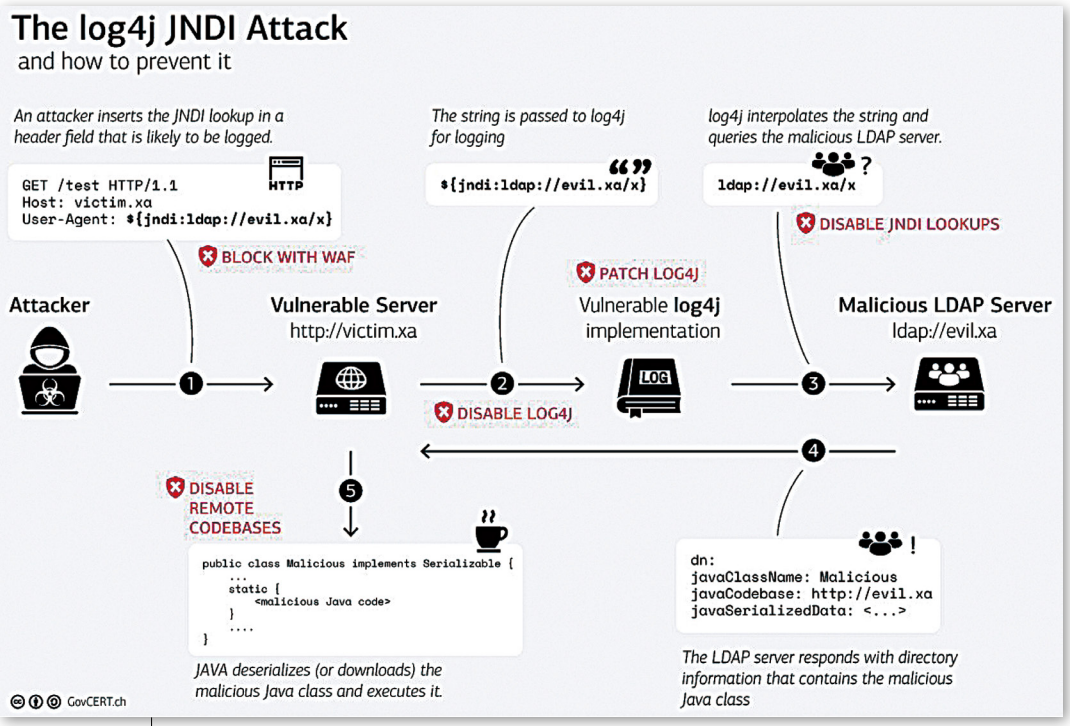
美國頒布 EO-14028 行政命令與推廣軟體物料清單（Software Bill of Materials, SBOM），藉此提高自身軟體供應鏈安全，進而協助國家關鍵基礎設施提升資安管理機制，其相關法制及政策值得我國借鏡與推廣。

關鍵設施軟體供應鏈安全日益重要

2020 年 SolarWinds 事件，駭客通過對雲端服務業者實施供應鏈攻擊，造成美國政府和工業部門機密資料重大外洩，2021 年 11 月 Log4j 漏洞（CVE-2021-44228）事件，造成美國金融業者至少 400 多萬客戶之重要金融資料被竊。[1] 2021 年 5 月，美國最大油管公司 Colonial Pipeline 遭勒索軟體攻擊，緊急關閉部分管道與 IT 系統，造成營運嚴重停擺。[2] 相關案例使各界重視軟體供應鏈安全，由於現今開源軟體大量應用，資訊專案軟體組成高度複雜，國家關鍵基礎設施之軟體安全，便格外受到矚目。

[1] 2021 年 12 月，廣泛出現於各應用程式的 Apache Log4j Java 有重大遠端執行漏洞，造成攻擊者能完全控制受影響系統。影響包括微軟 Minecraft、蘋果 iCloud、Steam 等大型網站，Tenable 稱其為 10 年來最嚴重之漏洞。

[2] 周峻佑，〈資安一周第 145 期：燃油供應商 Colonial Pipeline 遭勒索軟體攻擊，美國宣布進入緊急狀態〉，《iThome》，2021 年 5 月 11 日，https://www.ithome.com.tw/news/144342。



2021 年 11 月 Log4j 漏洞事件，造成美國金融業者至少 400 多萬客戶之重要金融資料被竊。（Photo Credit: GovCERT.CH, https://www.ncsc.gov.ie/emailsfrom/Reports/Log4j）

2021 年 5 月，美國最大油管公司 Colonial Pipeline 遭勒索軟體攻擊，造成營運嚴重停擺。（Photo Credit: Famartin, https://w.wiki/4qej）

美國政府重要政策

2021 年 5 月 12 日，美國總統拜登公布「改善國家網路安全的行政命令」（Executive Order on Improving the Nation's Cybersecurity, EO-14028），[3] 其中針對商業軟體開發因缺乏透明度、難以防止惡意行為者篡改等問題，實施更嚴格的安全維護機制。該命令要求美國網路安全及關鍵基礎設施安全署（Cybersecurity and Infrastructure Security Agency, CISA）等主管機關，應定期發布安全指引，增強軟體供應鏈之安全性。[4]

EO-14028 行政命令要求之重點 [5]

一、EO-14028 要求確保 IT 服務提供者能夠與聯邦政府分享資訊，尤其針對重大違規的資訊。

二、要求實施更嚴格網路安全標準，強化雲端服務保護和推展零信任架構，在特定時間內部署多因子驗證和加密措施。

三、要求銷售予政府軟體開發者應建立基本的軟體安全標準，包含開發人員應對其開發之軟體內容，保有更高的可見性（visibility），以及持續確保外界得以公開取得與其相關之軟體資訊。

[3] The White House, "Executive Order on Improving the Nation's Cybersecurity", May 12, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity.

[4] EO-14028 適用範圍為 FCEB 之聯邦部門（Federal Civilian Executive Branch），不包含國安、國防與情治單位。

[5] CISA, "Executive Order on Improving the Nation's Cybersecurity", https://www.cisa.gov/topics/cybersecurity-best-practices/executive-order-improving-nations-cybersecurity.

四、設立網路安全審查委員會，由政府和私部門負責人共同主持。委員會有權在重大網路事件發生後召開會議，分析原因並提出改善建議。

五、建立標準化手冊，確保所有聯邦機構符合一定的技術門檻，並採取一致性步驟來識別和減緩資安威脅。另強化聯邦政府內之端點偵測和回應（Endpoint Detection and Response, EDR）系統，並改善資訊分享機制以提升網路安全能力。

六、要求聯邦制訂網路安全事件日誌之規範，以提高有關入侵偵測、緩解駭侵行為以及認定資安事件程度的能力。

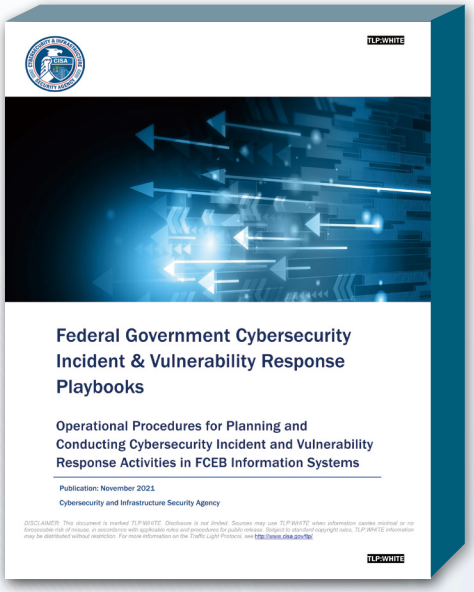
另為確保聯邦政府軟體供應鏈安全，EO-14028 要求採取下列措施：[6]

一、聯邦政府應推廣採用自動化工具或類似流程，來維護可信任之原始碼供應鏈，進而確保其完整性。

二、採用自動化工具或類似之流程來檢查已知與潛在漏洞並進行修復，該工具或流程應定期運作，或至少在產品、版本或更新發布前運作。

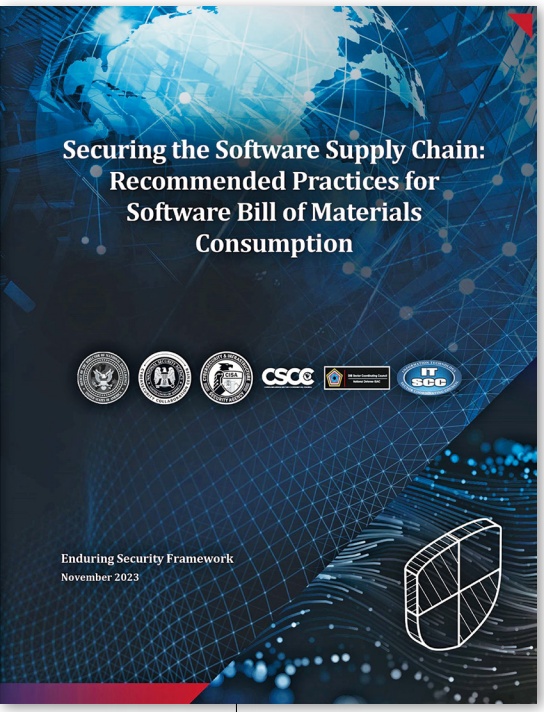
三、為促進開發商和供應商提供更安全的供應鏈，應採行於網站上發布等公開等方式，向購買者提供產品或資訊專案之「軟體物料清單」。

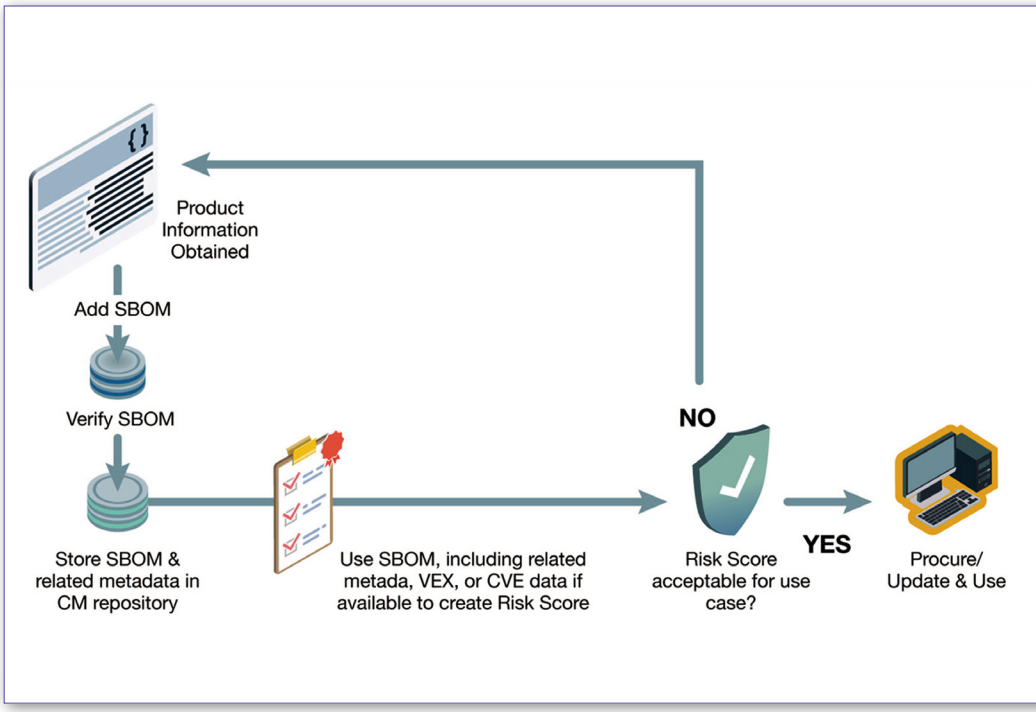
EO-14028 行政命令設立網路安全審查委員會，由政府和私部門負責人共同主持。（Photo Credit: Homeland Security twitter, https://twitter.com/DHSgov/status/1489254258897666055）



EO-14028 行政命令建立標準化手冊，確保聯邦機構符合一定的技術門檻，並採取一致性步驟來識別和減緩資安威脅。（Source: CISA, https://cisa.gov/sites/default/files/2024-03/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf）

[6] 參見EO-14028, Sec. 4. Enhancing Software Supply Chain Security, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity.





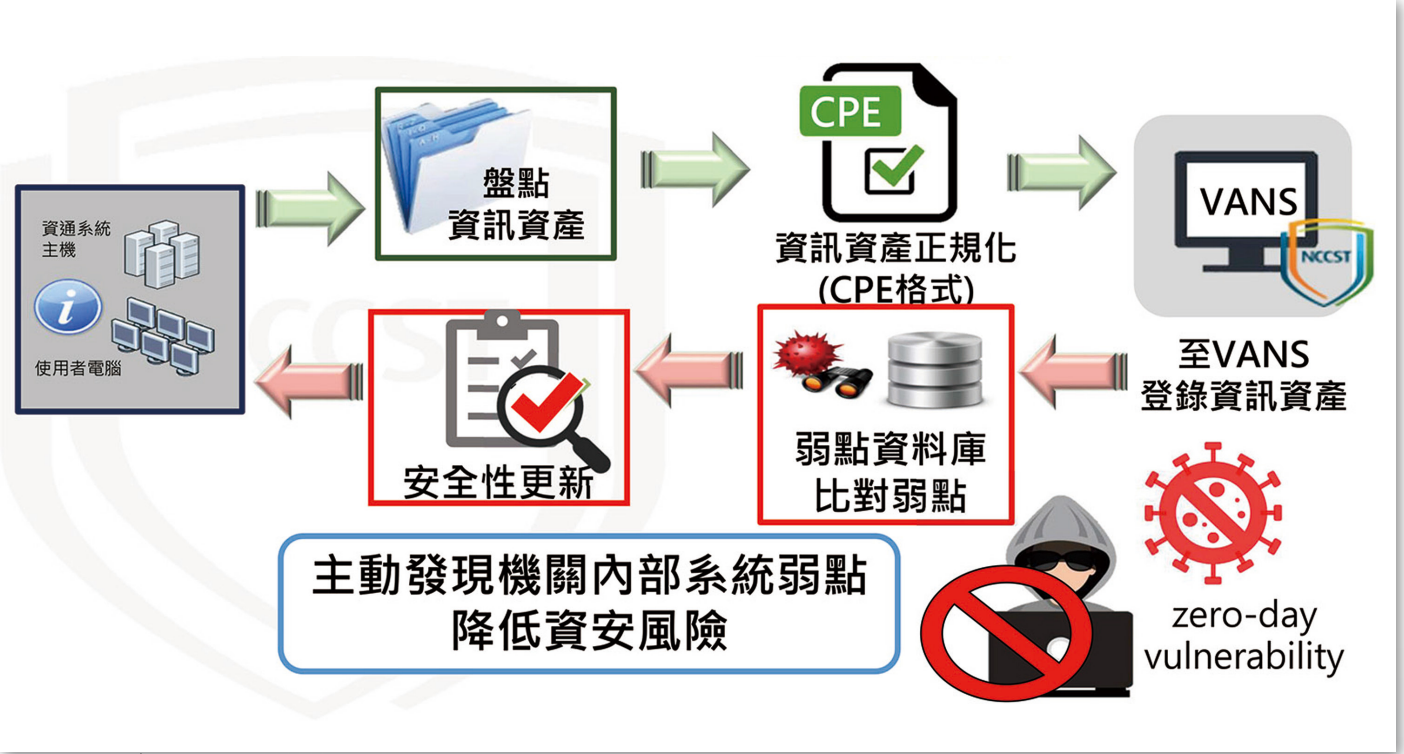
美國政府於 2023 年 11 月公布「保護軟體供應鏈：軟體物料清單的實踐建議」，協助使用者完成軟體之採購、測試、資安部署和軟體修補的建議流程，SBOM 具有即時更新組件內容與呈現完整資訊的效果，對降低攻擊風險有益。（Source: U.S. D.O.D, https://media.defense.gov/2023/Nov/09/2003338086/-1/-1/0/SECURING%20THE%20SOFTWARE%20SUPPLY%20CHAIN%20RECOMMENDED%20PRACTICES%20FOR%20SOFTWARE%20BILL%20OF%20MATERIALS%20CONSUMPTION.PDF）

軟體物料清單（SBOM）

軟體物料清單類似於軟體的「成分清單」，包含該軟體所有的基礎組件（component），都必須遵循既定的、機器可讀取的模式記錄，以標準化形式呈現其資訊。CISA、國家安全局（National Security Agency, NSA）和國家情報總監辦公室（Office of the Director of National Intelligence, ODNI）組成一個跨部門、公私合作的安全框架工作小組，並在 2023 年 11 月 9 日公布「保護軟體供應鏈：軟體物料清單的實踐建議」，以因應 EO-14028 對聯邦政府應提高軟體供應鏈安全性之要求，協助使用者完成軟體之採購、測試、資安部署和軟體修補的建議流程，並開發 SBOM 內容，以促進軟體資訊公開與漏洞即時修補。[7]

美國政府藉由 EO-14028 法案，對聯邦政府與企業界提高資安水準要求，並透過 SBOM 機制協助管理，讓使用者可對新出現的資安威脅快速反應，無須被動等待軟體商通知。另因 SBOM 具有即時更新軟體組件內容與呈現完整資訊的效果，對於降低零日漏洞攻擊風險，以及確保軟體符合智慧財產權規範等皆有助益，因此成為現今軟體安全和供應鏈風險管理的關鍵因素。

[7] CISA, "CISA, NSA, and Partners Release New Guidance on Securing the Software Supply Chain", November, 9, 2023, https://www.cisa.gov/news-events/alerts/2023/11/09/cisa-nsa-and-partners-release-new-guidance-securing-software-supply-chain.



由國家資通安全研究院管理之「資通安全弱點通報系統」可供機關登錄資訊資產、自動比對弱點資料庫，以協助機關確認其資訊資產是否存在公開漏洞。（資料來源：國家資通安全研究院，https://download.nics.nat.gov.tw/UploadFile/vans/ 資通安全弱點通報機制推廣說明 v1.0_1100609.pdf）

我國相關法制措施

我國近年依《資通安全管理法》及施行細則，要求政府與企業依循「事前規劃」、「事中維運」及「事後改善」等階段，落實安全維護計畫、改善資安缺失，並制度化鼓勵情資分享與公私合作；另公告「各機關對危害國家資通安全產品限制使用原則」、「政府資訊服務委外管理規定」、「政府資訊服務採購作業指引」等規定，試圖從法規面降低軟體供應鏈可能之資安風險。此外，由「國家資通安全研究院」管理之「資通安全弱點通報系統」（Vulnerability Analysis and Notice Service, VANS），可供機關登錄資訊資產、自動比對弱點資料庫，以協助機關確認其資訊資產是否存在公開漏洞。該系統預計擴充納入 SBOM 比對功能，未來將可供機關登錄並進行弱點比對及通報，由制度面強化資訊資產之風險管理。

結語

提高國家關鍵基礎設施軟體供應鏈之安全性，已是刻不容緩的任務。期待未來借鏡美國有關法規與政策，持續推動我國 SBOM 系統並健全國家關鍵基礎設施之資安管理機制。

從傳統反應性數位鑑識提升至主動式數位鑑識機制之探討
—以 DEFSOP 與 ISO27035 為例

◆ 大同大學資工所教授、台灣數位鑑識發展協會理事長 — 林宜隆、元盾資安公司執行長 — 趙永弘

隨全球資安議題日益嚴重，政府與企業強化資通設備安全性及優化數位鑑識技術亦日顯重要，為因應此挑戰，主動式數位鑑識機制（Proactive Digital Evidence Forensics Standard Operation Procedure, P-DEFSOP）應運而生，透過多樣的工具找出關鍵數位證據，並結合 MITRE ATT&CK 攻擊框架與 SIEM 和 MDR 工具，提供全面安全威脅偵測與分析，特別是雲端環境下，更需要公正性及有效性的數位鑑識服務（Digital Forensics Service）。主動式數位鑑識機制能有效提供全面的安全威脅偵測、分析與資安鑑識管理對策，並確保數位證據的法庭可接受性及完整性。

前言

大部分駭客入侵都無法有效阻擋，因為駭客藉系統漏洞、釣魚方法、社交工程多種攻擊手法，讓資訊安全管理人員防不勝防。大部分使用者或是公司企業，因為許多原因無法做到電腦即時更新，造成系統存在已知系統漏洞，提高了企業的資安風險。為了避免遭駭侵，我們應清楚了解其行為與方法，並思考如何降低損失；透過 MITRE ATT&CK 檢測技術與數位鑑識的檢測規則，相互對應檢視駭客留下怎樣的數位證據以及駭侵的手法，不僅可了解電腦受損程度，也能藉此提高警覺。

主動式數位鑑識技術（Proactive Digital Forensics Technology, PDFT）雖為資訊安全領域的重要趨勢之一，但其仍存在證據保全不足的問題，當 PDFT 搜集到證據後，仍需進一步確保其可作為法律證據。因此，需要強化保全證據之功能，例如加密、數位簽章、存儲安全，或儲存至區塊鏈，以確保證據不被篡改或洩露之技術。

主動式數位鑑識技術的發展和應用

「數位鑑識」（Digital Forensics）可定義為：利用科學驗證的方式調查數位證據，經由數位證據的擷取、分析、還原等過程，還原事件原貌，以利事件調查，並提供法庭訴訟之完整依據。「行動鑑識」（Mobile Forensics）屬於數位鑑識的其中一部分，指所有對行動裝置上的數位資料進行保存、識別、萃取、分析及鑑定的行為。

「資安鑑識」（Cyber Forensics）則為筆者所提出之概念，廣義領域包括「資安預防（Prevention）、資安防護（Protection）、證據保全（Preservation）及專業鑑識（Presentation）」等四大階段，並由澳洲 Jill Slay 教授與筆者共同提出 4P's Model 理論：要具備強大資安鑑識能量，其應包括符合 ISO 標準之 CyberLab 實驗室、標準作業程序 SOP、以及國際專業鑑識人才等。

「主動式數位鑑識」（Proactive Digital Forensics, PDF）是一種嘗試在數位罪行或事件發生之前就開始搜集可能證據的鑑識方法。與傳統的「反應性數位鑑識」（Reactive Digital Forensic, RDF）不同，主動式數位鑑識主要針對可能發生的事件進行預先的偵測和分析，從而提供預防罪行或其他惡意行為的機會。（圖 1）[1]

傳統反應性數位鑑識通常是對已發生的事件做出反應，事件發生後，鑑識專家會搜集硬碟、記憶體快照、日誌文件等數位證據。分析過程通常在事件發生後的一段時間內進行，並且可能會涉及大量的數位證據（或稱電子證據），但由於是在事後進行，所以對於防止未來事件發生的幫助有限。

[1] Soltan Abed Alharbi, Jens H. Weber-Jahnke, Issa Traore, *The Proactive and Reactive Digital Forensics Investigation Process: A Systematic Literature Review*, Information Security and Assurance - International Conference Proceedings, ISA 2011, Brno, Czech Republic, August 15-17, 2011.

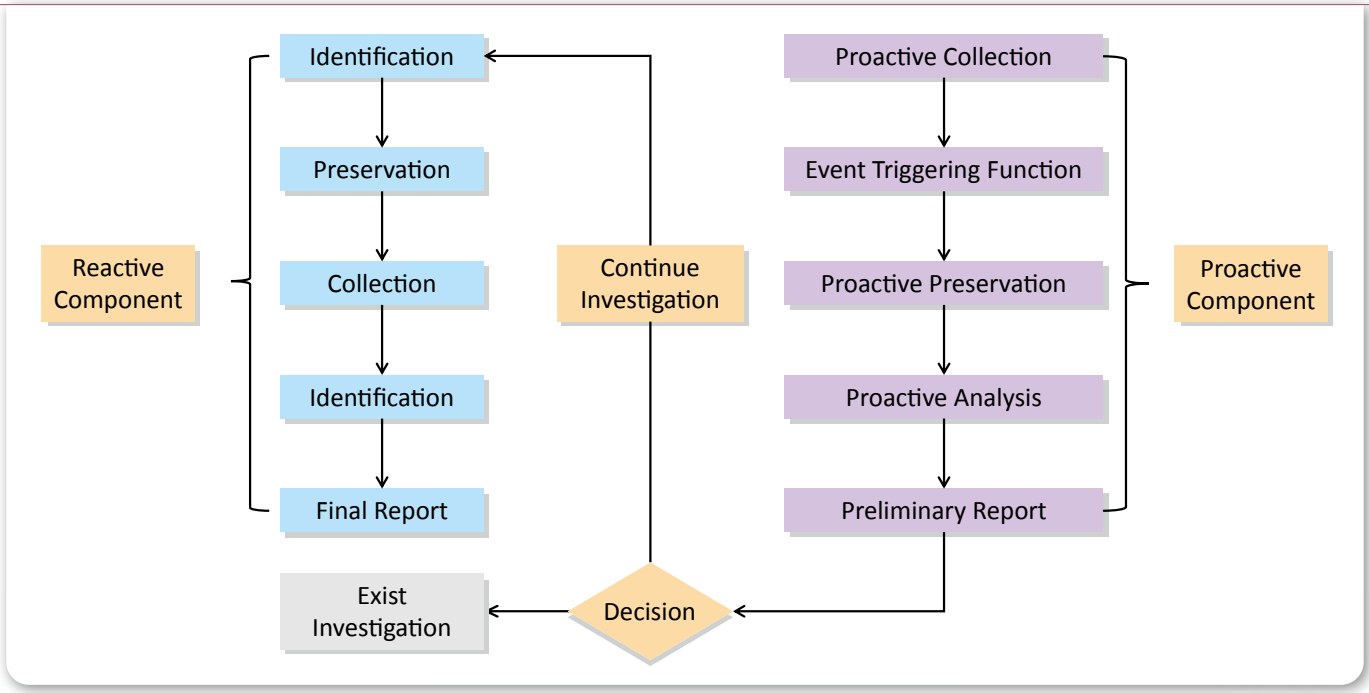


圖 1　主動／反應數位鑑識流程

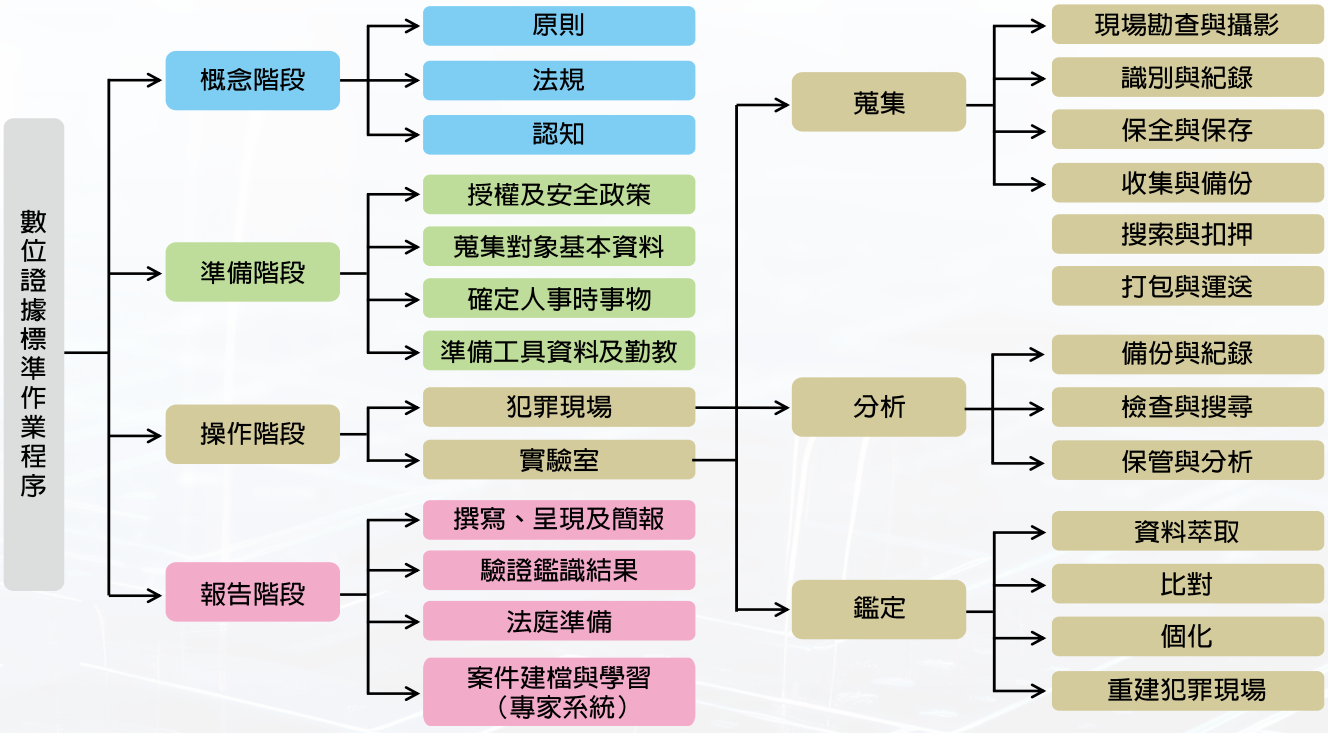


圖 2　數位證據鑑識標準作業程序（DEFSOP）

主動式數位鑑識能提供另一種防禦機制，來對抗日益複雜的網路攻擊。筆者提出的數位證據鑑識標準作業程序（DEFSOP，圖 2）以及主動式數位證據鑑識標準作業程序（P-DEFSOP），將鑑識過程分為概念、準備、操作、報告四個階段（圖 3）[2]，以清晰、條理化資安事件的處理過程。

[2] 林宜隆，〈建立整合性行動鑑識標準作業程序（iDEFSOP-MF）與實際案例驗證之研究—以刑事警察局破獲之實際案例及驗證為例〉，《刑事政策與犯罪研究論文集》，22 集，頁 361-404，筆者整理。

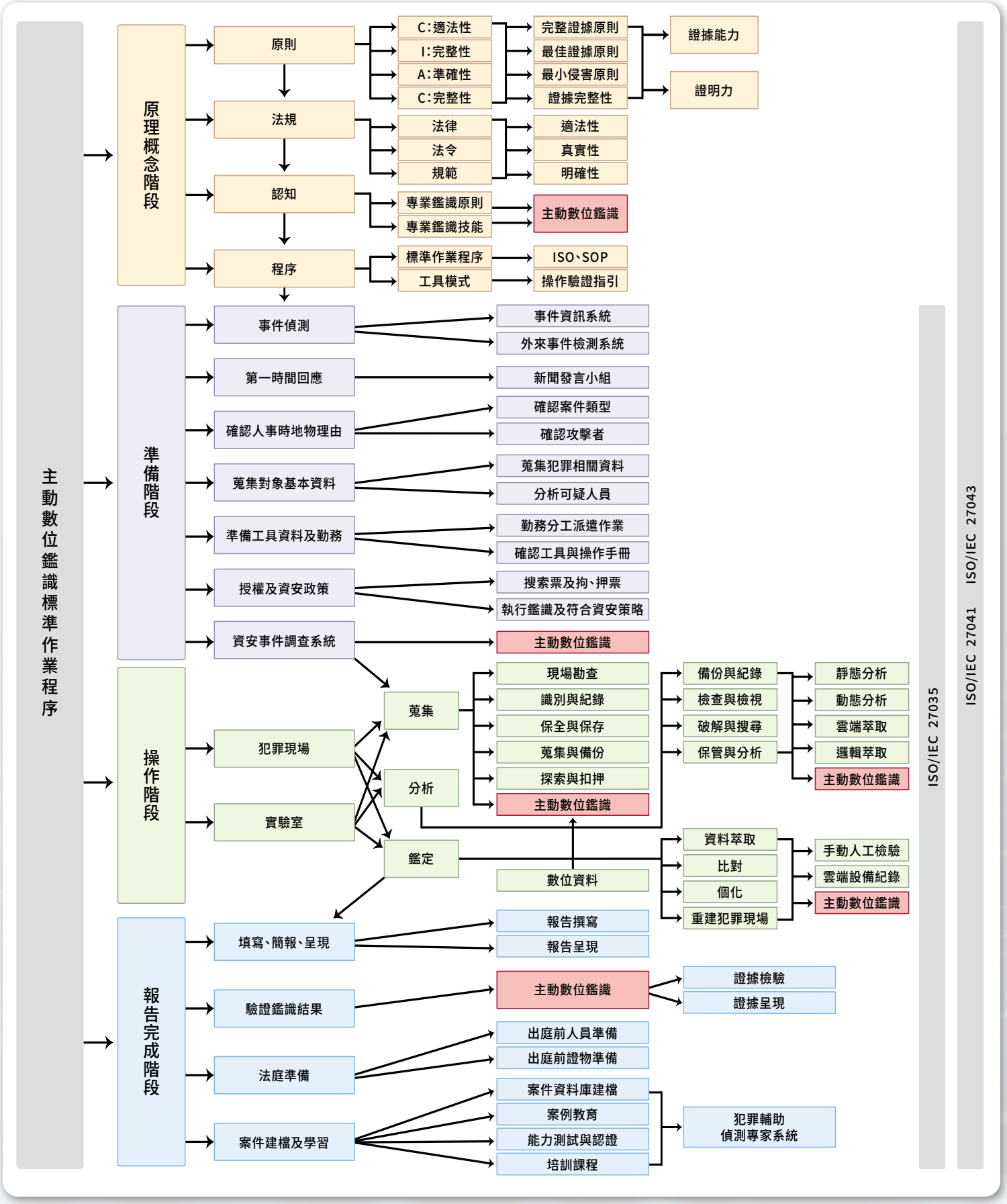


圖 3　主動式數位證據鑑識標準作業程序（P-DEFSOP）

國際資安事件管理標準
ISO/IEC 27035

ISO/IEC 27035 標準是一個國際資訊安全事件管理規範，提供應對資訊安全事件的統一、全面和可靠的框架。此標準強調資訊安全事件的生命周期管理，包括預防、準備、識別、評估、調查、解決和記錄等各個階段（圖 4）。

◆**預防階段**：通過實施安全措施和控制來減少資訊安全事件的發生。

◆**準備階段**：制定相應的應急計劃和程序，確保組織能夠有效應對事件。

◆**識別階段**：及時識別和評估事件的嚴重性和影響。

◆**調查階段**：進行資訊安全事件的調查，確定事件的原因和來源。

◆**解決階段**：採取適當的措施解決事件，恢復系統運作。

◆**記錄階段**：記錄事件的詳細資訊、處理過程和學習經驗，以便日後參考和改進。

通過遵循 ISO/IEC 27035 標準，可以建立一套有序、靈活且適應性強的資訊安全事件管理機制，以應對各種資訊安全事件。

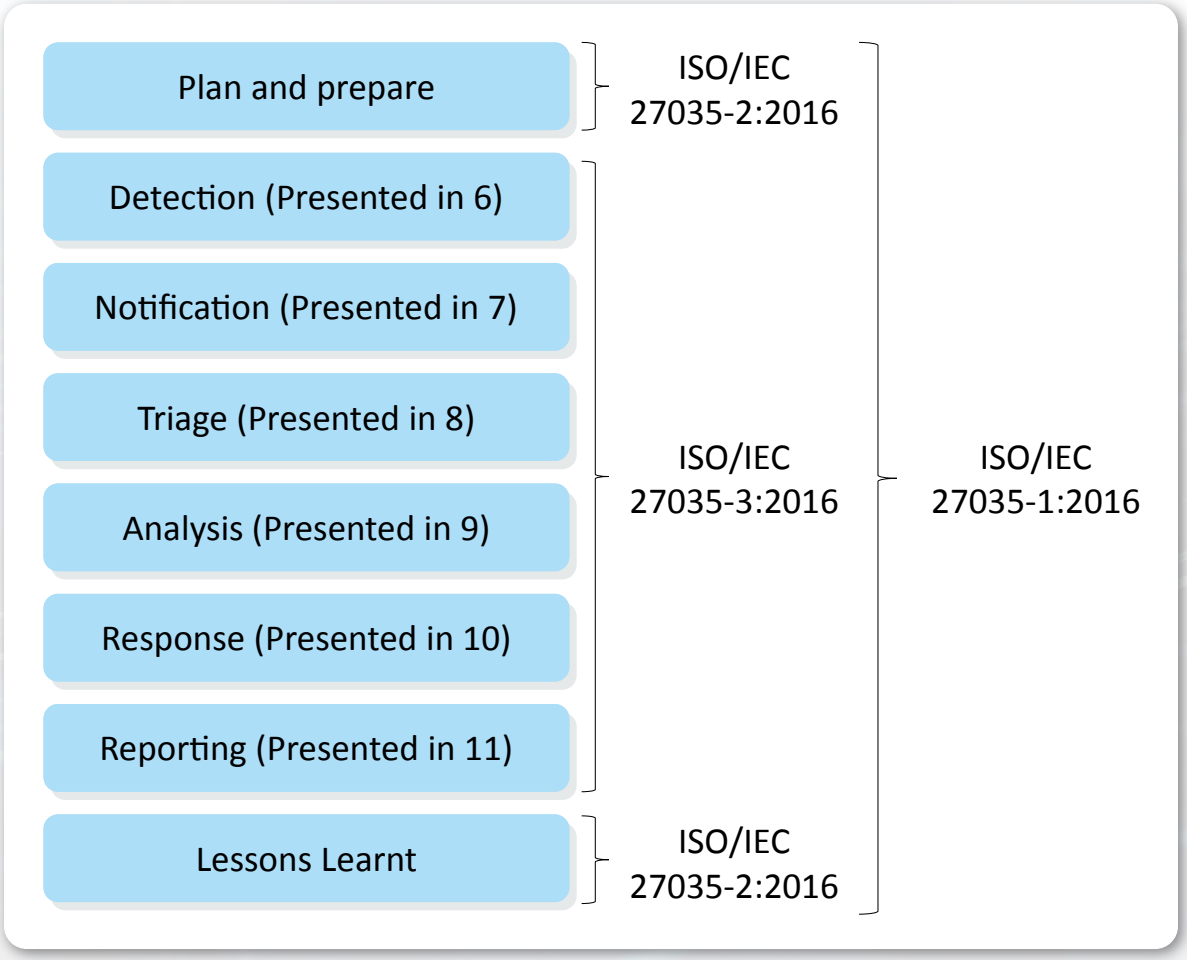


圖 4　ISO/IEC 27035 事件應變操作程序圖

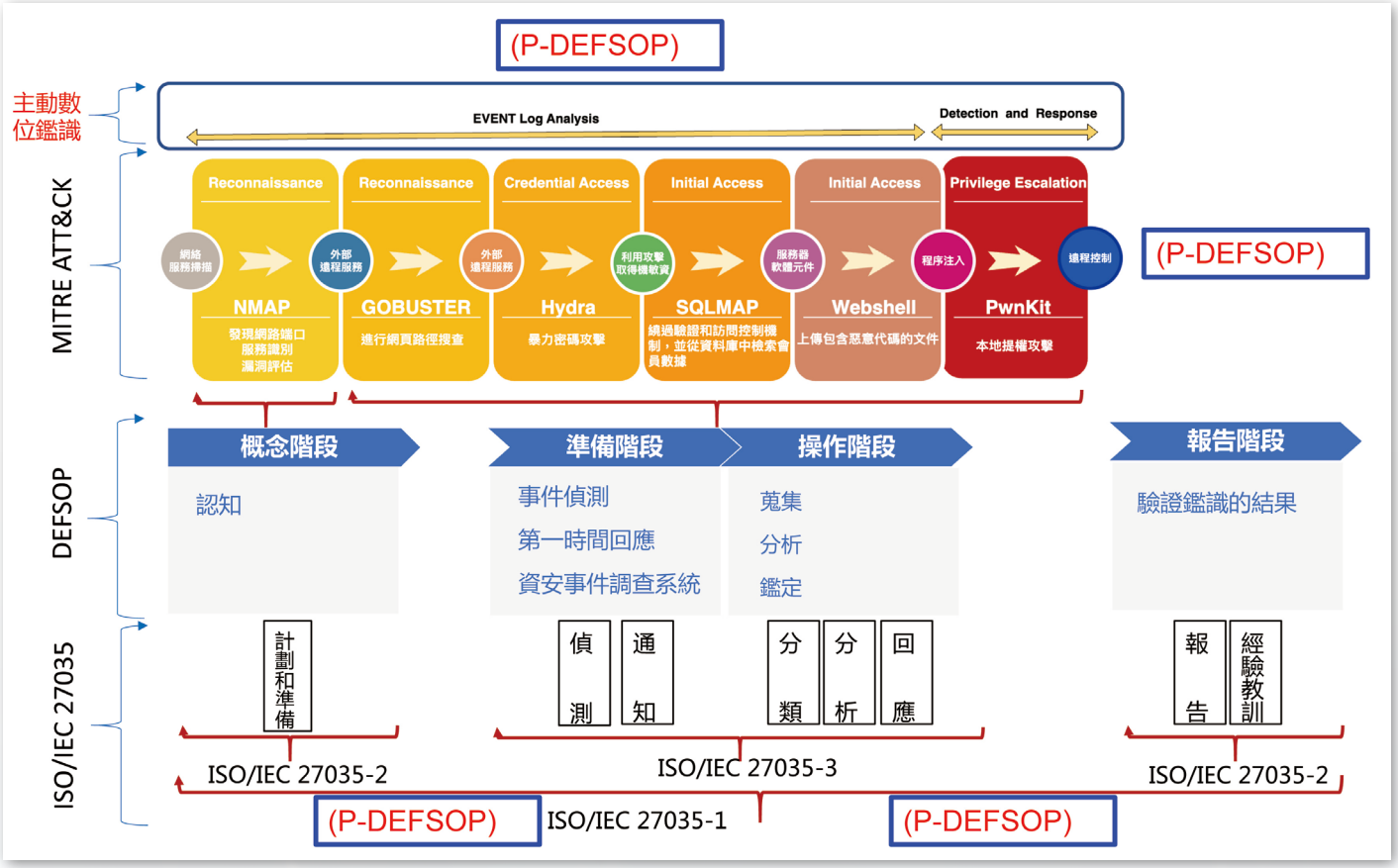


圖 5　主動式數位鑑識方案（P-DEFSOP）

依 ISO/IEC 27035 標準對應 P-DEFSOP，分析以 ManageEngine 的 EventLog Analyzer 作為安全資訊和事件管理（Security Information and Event Management, SIEM）系統是否符合國際標準，如圖 5 的主動式數位鑑識方案（P-DEFSOP）所示。

◆資訊安全事件管理分析

ISO 27035：5.3.3 資訊安全事件管理程序

EventLog Analyzer Server 功能：追蹤並記錄資訊事件，並提供警示及通報功能

◆安全審計軌跡分析

ISO 27035：6.1.3 安全審計軌跡

EventLog Analyzer Server 功能：收集系統事件、流量、應用程式等多種數據，並提供報表功能

◆準備應急處理計畫分析

ISO 27035：8.2.1 準備應急處理計劃

EventLog Analyzer Server 功能：提供告警、通報功能，並支援自動化反應和應急響應

◆安全測試分析

ISO 27035：9.2.2 安全測試

EventLog Analyzer Server 功能：提供網路和應用程式測試、漏洞掃描等功能，並更新相關攻擊資料庫，新增相關攻擊手法

◆資訊安全事件記錄分析

ISO 27035：12.2.1 資訊安全事件記錄

EventLog Analyzer Server 功能：收集、記錄、分析和查看資訊事件記錄

◆監測與測量分析

ISO 27035：13.2.1 監測與測量

EventLog Analyzer Server 功能：提供監測和測量功能，以收集器進行設備搜集資訊，異常時會主動通報

綜上可知，EventLog Analyzer Server 符合 ISO 27035 和數位鑑識 SOP 的理念，具備提供如資訊安全事件管理、安全審計軌跡、準備應急處理計劃、安全測試、資訊安全事件記錄和監測與測量等多種功能和工具之功能，可協助組織實現安全監控和事件管理。

結論

國際資安標準 ISO/IEC 27035 和數位鑑識 SOP 為資訊安全事件處理提供了一個清晰、有條理的框架，其原則能夠有效協助組織應對可能發生的資安事件，及提出應急管理對策，可以有效地防止個資外洩。

遵循國際資安標準 ISO/IEC 27035 和數位鑑識 SOP 的原則與程序，有助於組織在法律途徑中提升證據的有效性，也能協助掌握可疑的攻擊，達到預防勝於治療之目標。組織如適當地應用 ISO/IEC 27035 和數位鑑識 SOP，應可確保資安事件得到適時處理，減輕損失和風險，並有效保護組織的資訊資產。

個資保護 疑義解析

◆ 經濟部智慧財產局政風室主任 — 李志強

《個人資料保護法》（下稱個資法）自 101 年 10 月 1 日第 1 次修法上路以來，雖歷經 3 次修正，惟在實務上仍有諸多疑義。

重要實務見解

一、加密個資屬於《個資法》保護範圍

加密後之資料雖不能直接識別特定當事人，但若可對照、組合、連結識別特定個人，仍屬《個資法》所稱之個資。如金融機構上載經加密之自然人存款餘額查詢結果至財金公司之平臺暫存，再由行政執行署透過應用程式介面 API 介接，即時或批次自平臺取得資料及進行解密，即使因加密而無法知悉其內容，但該餘額查詢結果仍屬經對照、組合或連結後，得以識別特定當事人者，仍屬《個資法》之個資。

二、消費者信用卡卡號屬於《個資法》保護範圍

依據《個資法》第 2 條第 1 款規定，個資指自然人之姓名……及其他得以直接

加密資料雖無法直接識別特定當事人，但若可對照、組合、連結識別特定者，仍屬《個資法》所稱之個資。

店家欲透過取得消費者信用卡卡號以確認特定自然人身分，屬《個資法》上蒐集個資行為，應符合《個資法》第 19 條第 1 項有關蒐集個資合法事由規定。

或間接方式識別該個資；另同條第 3 款規定，蒐集指以任何方式取得個資，如店家欲透過取得消費者信用卡卡號以確認特定自然人身分，屬《個資法》上蒐集個資行為，自應符合《個資法》第 19 條第 1 項各款有關非公務機關（指公務機關以外之自然人、法人或其他團體）蒐集個資合法事由規定。

非公務機關向當事人蒐集個資時，除有《個資法》第 8 條第 2 項得免為告知之情形者外，應依法履行告知義務，告知方式得以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之，而告知方式亦非以書面為限，且未要求當事人簽署。

三、個資當事人得授權他人代為行使其權利

個資當事人對保有其個資之公務機關或非公務機關有查詢、請求閱覽之權利，除有《個資法》第 10 條但書所列得拒絕提供之情形者外，前述機關應依當事人請求，就所蒐集之當事人個資答覆查詢、提供閱覽。另依《民法》第 103 條第 1 項規定，代理人於代理權限內，以本人名義所為之意思表示，直接對本人發生效力。故當事人自得授權其代理人行使上開權利，惟有關代理權限之有無及其範圍，則屬個案事實認定。

四、檢舉人不得要求公務機關提供被檢舉人違反行政罰之受裁罰法條及罰鍰金額

《個資法》第 3 條第 1 款係保障個資當事人對其個資之使用有知悉權，僅由該筆個資之當事人所享有，亦即僅賦予個資之本人查詢、閱覽及複製其個資之權利，並未賦予人民得請求公務機關提供他人個資之權利。公務機關蒐集、處理被檢舉人裁罰之相關資料，原係基於行政裁罰、行政調查之特定目的，如擬提供非該裁罰案件之當事人查詢，則屬特定目的外之利用，應有《個資法》第 16 條但書所列各款情形之一（如法律明文規定、經當事人同意等），始得為之。

五、公務機關或非公務機關不得逕依當事人請求即刪除其個資

《個資法》第 3 條第 5 款僅規定當事人就其個資之刪除權不得預先拋棄或限制，有關當事人行使刪除其個資之權利，仍應依《個資法》第 11 條第 3 項規定辦理，亦即個資蒐集之特定目的消失或期限屆滿時，應主動或依當事人之請求，刪除、停止處理或利用該個資，但因執行職務或業務所必須或經當事人書面同意者，不在此限。有關前項但書於《個資法施行細則》第 21 條明定 3 種情形：（一）有法令規定或契約約定之保存期限；（二）有理由足認刪除將侵害當事人值得保護之利益；（三）其他不能刪除之正當事由。

如蒐集個資之特定目的消失或期限屆滿時，當事人就其個資雖有請求刪除之權利，惟「有法令規定之保存期限」，公務機關或非公務機關仍得拒絕當事人刪除之請求，上述保存期限宜注意《個資法》第 5 條比例原則，避免對於個資為不必要之蒐集、處理或利用。

六、公務機關不得請電信公司提供行動用戶資料進行電話訪問

依據司法院釋字第 631 號解釋理由書，《憲法》第 12 條規定人民有秘密通訊之自由，……國家若採取限制手段，除應有法律依據外，限制之要件應具體、明確，不得逾越必要之範圍，所踐行之程序並應合理、正當。如《電信法》第 7 條第 1 項規定，電信事業或其服務人員對於電信之有無及其內容，應嚴守秘密；另《電信管理法》第 9 條第 1 項亦明文，電信事業對於用戶之通信紀錄及帳

《個資法》第 3 條第 1 款係保障個資當事人對其個資之使用有知悉權，僅由該筆個資之當事人所享有，即僅賦予個資本人查詢、閱覽及複製其個資之權利，未賦予人民請求公務機關提供他人個資之權利。

電信公司所掌有之行動電話用戶資料係屬人民秘密通訊自由之基本權保障範疇，依《電信法》和《電信管理法》規定，電信事業或其服務人員對於通信內容及帳務紀錄等，負有保密義務。

務紀錄，應予保密。準此，電信公司所掌有之行動電話用戶資料係屬人民秘密通訊自由之基本權保障範疇，電信事業負有保密義務。

依《個資法》第 5 條規定，公務機關或非公務機關蒐集、處理或利用個資應符合比例原則之要求，其所採取之方法應有助於目的之達成（適當性），應選擇對人民權益損害最少（必要性或侵害最小性），且對人民權益造成之損害不得與欲達成目的之利益顯失衡平（衡量性或狹義之比例原則）。

綜上，為保障人民秘密通訊自由，且電信公司對於行動電話用戶資料應負保密義務，故電信公司不得提供相關資料使公務機關進行電話訪問，而公務機關雖得以蒐集或處理個資，然應以對個資當事人權益侵害較小之方式為之。故公務機關若請電信公司提供行動用戶資料進行電話訪問，已逾越執行法定職務之必要範圍。

七、業者以贈品誘使學童提供個資應善盡告知及取得同意

業者基於當事人同意，蒐集未成年學童之個資，除應注意以贈品誘使學童提供個資，是否已違反《個資法》第 5 條之誠實信用原則外；另應踐行《個資法》第 8 條第 1 項相關法定應告知事項，告知方式應符合學童之年齡、生活經驗及理解能力，以容易理解、清楚簡單之語言或文字為之，並使該學童得以充分瞭解其個資之後續利用，倘業者未完整踐行告知，或其告知對象無法充分瞭解其個資之後續利用，即不

業者蒐集未成年學童之個資，須踐行《個資法》相關法定之應告知事項，其方式應符合學童之年齡、生活經驗及理解能力，以容易理解、清楚簡單之語言或文字為之，並使其充分瞭解個資後續之利用。

符合《個資法》第 7 條第 1 項所稱同意之規定，而業者就當事人同意合法要件之事實亦應負舉證責任。

《個資法》第 7 條第 3 項明定，公務機關或非公務機關明確告知當事人第 8 條第 1 項各款應告知事項時，當事人如未表示拒絕，並已提供其個資者，推定當事人表示同意。是以，若業者欲透過「推定同意」之方式取得個資，除應盡告知義務且明確告知外，尚須符合「當事人未表示拒絕」及「當事人已提供其個資」兩項要件，始得為之。所謂「當事人未表示拒絕」，指當事人在正面選擇同意與否之模式下進行，否則有「預設同意」之虞；所稱「當事人已提供其個資」，係當事人有自行提供個資之積極行為，倘預設自動上傳而取得個資，縱當事人未表示拒絕，仍不符合推定同意之要件。此外，關於未成年人行使《個資法》上相關權利，應回歸適用《民法》有關行為能力之一般性規定。

八、公務機關調閱學員出入境資料似不符特定目的外利用之要件

《個資法》第 16 條但書第 4 款所稱「為防止他人權益之重大危害」屬不確定法律概念，應依具體個案情形認定之，例如醫院為免除病人生命、身體之危險，向戶政事務所請求提供無自主能力之患者親屬戶籍資料，以通知患者親屬協處相關事宜，若戶政事務所提供患者親屬戶籍資料，可認係為防止患者權益之重大危害。

公務機關蒐集、處理或利用個資，應符合《個資法》第 5 條及《行政程序法》第 7 條比例原則之要求，於執行法定職務「必要範圍內」為之，且不得逾越特定目的之「必要範圍」，而所採取之方法，應符合適當性、必要性及狹義之比例原則。是以，公務機關若為調查學員有無申請不實事假違反請假規定，並以避免影響學員全體權益及日後民眾權益等為由，請內政部移民署提供特定學員申請事假期間之出入境資料，藉以作為提報公務人員保障暨培訓委員會廢止該員受訓資格之關鍵證明文件，似未達「重大」危害之程度。

九、個人架設線上族譜網站並不適用《個資法》第 51 條排除條款

依《個資法》第 51 條第 1 項第 1 款規定，自然人為單純個人或家庭活動之目的，而蒐集、處理或利用個資，不適用《個資法》規定。其立法理由係自然人為單純個人（如社交活動等）或家庭活動（如建立親友通訊錄等）而蒐集、處理或利用個資，

公務機關若為調查學員有無違反請假規定，以避免影響學員全體權益及日後民眾權益等為由，請移民署提供特定學員之出入境資料，藉以作為相關證明文件，似未達「重大」危害民眾權益之程度。

自然人為單純個人或家庭活動目的而蒐集、處理或利用個資，不適用《個資法》規定；但若將資訊架設為網站公開予不特定人瀏覽，相關資料之蒐集、處理及利用則應按照《個資法》第 19、20 條規定辦理。

因屬私生活目的所為，與其職業或業務職掌無關，如納入《個資法》之適用，恐造成民眾之不便亦無必要，爰予以排除。

若個人架設線上族譜網站雖與其職業或業務無關，惟該網站係供不特定人瀏覽，且內容涉及族譜成員之工作地、配偶、子女、戶籍地址及連絡電話等詳細資料，此依《個資法》第 5 條規定，恐已逾越單純個人或家庭活動目的之必要範圍，而難認有《個資法》第 51 條之適用，故相關資料之蒐集、處理及利用應依《個資法》第 19、20 條規定（如經當事人同意）辦理。

結語

誠如司法院大法官所見，隱私權為不可或缺之基本權利，故屬《憲法》所保障者，其中就個人自主控制個資之資訊隱私權而言，乃保障人民決定是否揭露其個資、及在何種範圍內、於何時、以何種方式、向何人揭露之決定權，並保障人民對其個資之使用有知悉與控制權及資料記載錯誤之更正權。透過本文可知，個資保護並非僅是法令條文，而是攸關每個人權益，大眾均應建立正確認識並且知法守法。

怕熱的岩大戟和它們的朋友

翠綠的岩大戟

◆ 文字、攝影／林業試驗所 — 徐嘉君

臺灣東北角龍洞除了是攀岩聖地，也是觀察許多稀有岩生植物的好地方，晚春是這裡最熱鬧的季節，除了張狂如繁星的石板菜以外，最翠綠可愛的便是岩大戟了，岩大戟很怕熱，到初夏5月，葉色就會轉紅準備休眠。忽然發現大快朵頤後準備羽化的大笨蝶，那金光閃閃的蛹殼也是同色系呢。

大笨蝶金色的蛹

明亮如繁星的石板菜

歸來牛蒡

◆ 文史工作者 — 蘇箏

牛蒡具豐富的胺基酸，有蔬菜之王的美稱，在日本的飲食文化中，幾乎與健康養生畫上等號，每個家户都懂得善用這種保健蔬菜。

牛蒡的原鄉

屏東縣歸來地區，栽種生產品質最上等的「大力蔘」牛蒡，是在前行政院農業委員會、屏東縣政府與屏東市農會輔導推動下，由一群志同道合的農家歸來學子，組織屏東歸來社區發展協會，成立屏東市蔬菜產銷班第 13 班，完全採用有機肥料栽種方式共同開發研究的產品，經檢驗證明無農藥、無重金屬殘留，並取得吉園圃 GAP 與 CAS 雙重認證與生產履歷。

日治時期，日兵進駐臺灣，當時臺灣沒有種植牛蒡，又不可能從日本空運來臺，

屏東歸來是臺灣「牛蒡的原鄉」，該地區特有的「紅土沙」土質鬆軟、排水性良好，在此生長的牛蒡質地鮮嫩，營養成分豐富多樣。

由於牛蒡性喜溫涼，對土壤要求嚴格，需要排水良好的砂質土壤，日本政府派了一名農業博士來臺灣勘察，看有無適合種植牛蒡的地點，經日本農業專家勘查結果，竟意外發現歸來地區的土質為特有粘板岩老沖積土，即當地俗稱的「紅土沙」土質，主要以老下淡水溪（今高屏溪）、東港溪和林邊溪之沖積物沉積而成，其母質以粘板岩風化物為主，土質較為鬆軟，且排水性良好，從而雀屏中選，自此開啟臺灣種植牛蒡的歷史。

日本人將品系最佳的「柳川」品種牛蒡從日本引進屏東歸來栽培，在這樣環境成長的牛蒡品質，不僅質地鮮嫩，其營養和機能性成分亦多樣豐富，長期以來，外銷深受肯定，因此，牛蒡成為歸來地區特有農產品，亦使歸來地區成為臺灣「牛蒡的原鄉」。

日本人將品系最佳的「柳川」品種牛蒡引進屏東歸來栽培。

古籍與現代醫學中的珍品

牛蒡（Burdock root，日文：ごぼう）屬於寒性的食物，為菊科牛蒡屬草本植物，原產於歐洲、西伯利亞，之後才傳入亞洲，有吳帽、大力子、便牽牛、蒡翁菜、蝙蝠刺等多種別名，在古時還有另一個別名，稱作

「牛房」（即牛的尾巴）。又因根形似人蔘，而有「臺灣人蔘」、「大力蔘」、「最平價的人蔘」等美名，是蔬菜中的珍品。

牛蒡的獨特味道可與人蔘媲美，不但能當作藥材使用，也能加入菜餚中提升味覺豐富度。在日本料理中很常見到牛蒡，反映日人愛吃牛蒡的喜好，其被日人認為是蔬菜中營養價值非常完整的食材。因含有豐富蛋白質、醣類、膳食纖維、維生素群、胺基酸、礦物質及生理活性成分、菊糖、不飽和脂肪酸等，依《本草綱目》記載，牛蒡可「通十二經脈，洗五臟惡氣」及「久服輕身耐老」，有排毒、抗衰老與瘦身之意義，是營養與保健價值頗高的健康蔬菜。

牛蒡對於人體的益處很多，但並非每個人都適合吃牛蒡，舉例若有下列情形時，須盡量避免食用過多的牛蒡：

其一，腸胃不佳者：牛蒡的纖維豐富，在每 100 公克的牛蒡中，含有 5.1 公克的膳食纖維，含量是胡蘿蔔的 2.6 倍，花椰菜的 3 倍，雖然能促進腸胃蠕動，剛開始吃牛蒡的人，可能會出現輕瀉的情況，建議不要一次吃太多，以漸進式吃法逐漸增加份量；但若本身腸胃功能不佳者，尤其是腸胃道正在發炎的人，若食用牛蒡過量，容易出現脹氣、腹瀉、消化不良等腸胃症狀。

其二，腎功能不佳者：牛蒡中的鈣、鎂、鉀、鐵等微量元素含量豐富，鈣是維持骨骼密度、預防骨質疏鬆症的重要成分；鎂能幫助肌肉、穩定神經系統的正常運作；鉀則對需要利尿的患者有所助益；鐵是組成血液的成分，補充足量的鐵質，可降低

牛蒡原產於歐洲、西伯利亞，之後才傳入亞洲，因根形似人蔘，而有「臺灣人蔘」、「大力蔘」、「最平價的人蔘」等美名，是蔬菜中的珍品。

牛蒡富含各種營養成分，有排毒、抗老與瘦身之功效，為保健價值極高的健康蔬菜。

牛蒡對人體益處多，但仍需依個人體質調整食用量；圖為牛蒡烏龍麵、炒牛蒡、炸牛蒡等料理。

貧血的風險。但每 100 公克約含鉀 358 毫克，因此，若食用過量可能引發高血鉀症，並加重腎臟負擔。建議依個人體質調整食用量，或先諮詢醫師與營養師再食用。

傳承牛蒡好滋味

最近幾年，臺灣的經濟結構改變，在加入世界貿易組織 WTO、青年陸續轉業或外出謀生等條件衝擊下，歸來社區的傳統農業與現代發展逐漸顯得漸行漸遠，以致農村人口萎縮；為了從根本上找回昔日的精神與風華，牛蒡的推廣即成為復興歸來過往榮光的首要工作，父執輩的生活技藝，才得以讓居民傳承下去。

歸來社區第三代牛蒡達人陳姓農友有鑑於此，將傳統農業與生物科技產業結合，再創牛蒡經濟價值，帶著農民走出低迷景氣，營造「歸來牛蒡」自有品牌；歸來社區並與鄰近的技術學院合作，研發牛蒡的副產品（如牛蒡茶、茶包等），多元開發本土牛蒡市場，歡迎民眾多方嘗試。

歸來社區的農友致力於推廣牛蒡，並與產學單位合作，研發茶包、脆片、麵條等牛蒡副產品。

113 年法務部調查局調查人員特考（三等考試）

報名日期：113 年 4 月 30 日至 5 月 9 日（網路下載報名表／紙本寄件）
考試日期：113 年 8 月 10 日至 11 日（第一試筆試）
考試主辦機關：考選部（02-22369188 轉特考司）
報名書表（應考須知）：請於報名期間利用考選部網站下載報名

組別	第一試		第二試	第三試	備註
	普通科目	專業科目	體能測驗	口試	
調查工作組	一、國文（作文與測驗） 二、綜合法政知識與英文	三、社會學 四、政治學 五、刑法與刑事訴訟法 六、外國文（詳附註）	心肺耐力測驗 1,200 公尺跑走 ※ 及格標準 男性： 5 分 50 秒以內 女性： 6 分 20 秒以內	個別口試	1. 考試預定錄取名額以考選部正式公告為準。 2. 有關年齡、兵役及學歷等應考資格及應繳文件，可至考選部網站應考人專區下載本年度應考須知，內已詳載。 3. 相關法規：公務人員特種考試法務部調查局調查人員考試規則。
法律實務組		三、刑法 四、刑事訴訟法 五、行政法 六、商事法			
財經實務組		三、經濟學 四、財務管理 五、中級會計學 六、證券交易法與商業會計法			
化學鑑識組		三、生物化學 四、有機化學 五、分析化學 六、儀器分析			
醫學鑑識組		三、生物化學 四、有機化學 五、分子生物學 六、遺傳學			
電子科學組		三、電子學與電路學 四、計算機概論 五、工程數學 六、通信與系統			
資訊科學組		三、系統分析與設計 四、資料庫應用 五、資通網路 六、資訊安全實務			
營繕工程組		三、結構分析 四、營建法規 五、施工法 六、政府採購法			
附註：外國文選試科目（英文、日文、德文、西班牙文、阿拉伯文、法文、俄文、韓文、土耳其文）。					

各項考試資訊請參考考選部（https://www.moex.gov.tw）或法務部調查局（https://www.mjib.gov.tw）網站特考資訊專區，並以考選部正式公告為準。

邀稿說明

一、 清流雙月刊是法務部調查局所發行之「全國安全防護」宣導刊物，邀稿完全對外公開，歡迎踴躍投稿。

二、 本刊宗旨為宣導國家安全，投稿方向可參閱本刊的單元類別 ，或至法務部官網電子書櫃「清流雙月刊徵稿說明及訊息公告」查詢。

三、 本刊刊載以白話且易讀的文章為主，來稿字數以 2,000 字內為限，並請加註 60 字內摘要；若投稿為**主要業務**相關的文章，字數限制可調整至 3,000 字以內。本刊對來稿保有修改與增刪之權力。

四、 文章一經發表，其著作財產權即授權本刊，並同意經本局再行授權第三人利用，但作者仍保有著作人格權，保有該著作未來自行集結出版與教學等個人使用之權利。

五、 由於本刊為政府出版品，投稿文章需同時授權予政府出版品主管機關— 文化部以及文化部所授權之對象刊載。

六、 投稿文字請寄送至電子信箱：**2d40@mjib.gov.tw**，並留下聯絡電話及住址（未留聯絡方式、非電子檔形式之稿件及圖片，不予採用，亦不主動退回）由於本局信箱有單信最大容量上限（8MB），若投稿內容包括圖片等較大容量之檔案，請分封寄送。

七、 清流雜誌社聯繫方式請以電子郵件為主，寄至上述投稿信箱；若有急務請電 02-29112241 轉 3332 或 3333。

八、 本刊發行層面廣泛，致文章內容難以兼顧各界需求；若有價值觀或理念不同者，敬請讀者見諒。

電子書連結說明

電子書版本提供自動連結，點選後可連線至資料或影像來源，閱讀更多相關資訊。

友情陣線

海巡季刊　　移民雙月刊　　警光

讀者意見表

一、請問您從何處取得本刊？

☐ 我是訂戶　☐ 親友熟識推薦　☐ 公共場所、圖書館

☐ 其他 _____

二、您閱讀本刊的原因是？

☐ 訂戶定期閱讀　☐ 被封面吸引　☐ 喜歡某位作者或文章

☐ 其他 _____

三、您喜歡哪些美術編排？

☐ 封面　☐ 封底　☐ 目錄　☐ 主題文章

☐ 內文排版與圖片，頁數：_____

四、本期喜歡的單元是：

☐ 科技之島　站穩國際　☐ 放眼國際　☐ 無聲滲透　☐ 防恐任務

☐ CI 學堂　☐ 科偵世界　☐ 法令天地　☐ 絕美臺灣

☐ 飲膳札記　☐ 其他：_____

五、您的基本資料：

姓　名：　　電話 / E-mail：

住　址：

年　齡：○ 20 歲以下　○ 21-40 歲　○ 41-60 歲　○ 61 歲以上

學　歷：○ 國中以下　○ 高中職　○ 大學（專）以上　○ 碩士　○ 博士

職　業：○ 上班族　○ 軍公教　○ 學生　○ 家管　○ 已退休　○ 其他_____

※ 本刊依個人資料保護法及相關法令規定，所蒐集之個人資料僅做聯繫及相關合理應用。

其他建議：

_____

_____

_____

_____

電子版讀者意見表

e-mail：2d40@mjib.gov.tw

法務部調查局檢舉專用電話一覽表

機關名稱	地址	檢舉電話
法務部調查局	231209 新北市新店區中華路 74 號	（02）29177777 （02）29188888（傳真）
臺北市調查處	106229 臺北市大安區基隆路二段 176 號	（02）27328888
新北市調查處	220075 新北市板橋區漢生東路 193 巷 2 號	（02）29628888
桃園市調查處	330026 桃園市桃園區縣府路 19 號	（03）3328888
臺中市調查處	403012 臺中市西區英才路 525 號	（04）23038888
臺南市調查處	708008 臺南市安平區永華路二段 208 號	（06）2988888
高雄市調查處	801612 高雄市前金區成功一路 428 號	（07）2818888
航業調查處	435059 臺中市梧棲區臨港路四段 390 號	（04）26560555
福建省調查處	893017 金門縣金城鎮西海路一段 65 號	（082）322888
基隆市調查站	201005 基隆市信義區崇法街 220 號	（02）24668888
宜蘭縣調查站	260023 宜蘭縣宜蘭市津梅路 52 號	（03）9288888
新竹市調查站	300075 新竹市香山區經國路三段 126 號	（03）5388888
新竹縣調查站	302099 新竹縣竹北市光明五街 56 號	（03）5558888
苗栗縣調查站	360017 苗栗縣苗栗市玉清路 382 號	（037）358888
南投縣調查站	540019 南投縣南投市民族路 486 號	（049）2228888
彰化縣調查站	500034 彰化市卦山路 12 號	（04）7248888
雲林縣調查站	640013 雲林縣斗六市鎮南路 67 號	（05）5328888
嘉義市調查站	600011 嘉義市東區維新路 321 號	（05）2778888
嘉義縣調查站	613016 嘉義縣朴子市朴子一路 1 號	（05）3628888
屏東縣調查站	900044 屏東縣屏東市合作街 51 號	（08）7368888
花蓮縣調查站	970064 花蓮縣花蓮市中美路 3-33 號	（03）8338888
臺東縣調查站	950254 臺東縣臺東市中興路二段 731 號	（089）236180
澎湖縣調查站	880010 澎湖縣馬公市新明路 77 號	（06）9278888
馬祖調查站	209001 連江縣南竿鄉介壽村 15 號	（0836）22258
北部地區機動工作站	235028 新北市中和區永和路 33 號	（02）22482626
中部地區機動工作站	407003 臺中市西屯區福順路 500 號	（04）24615588
南部地區機動工作站	812003 高雄市小港區平和南路 129 號	（07）8122910
東部地區機動工作站	970018 花蓮縣花蓮市瑞美路 7 號	（03）823-3712
國家安全維護工作站	231206 新北市新店區中生路 40 號	（02）22177211
航業調查處基隆站	202007 基隆市中正區中正路 303 號	（02）24633633
航業調查處高雄站	806041 高雄市前鎮區佛公路 167 號	（07）8134888

調查局免付費「檢舉專線電話」— 0800-007-007

設定直接轉接至調查局北、中、南、東四個地區機動工作站及外島處站，值日人員 24 小時接聽受理

Happy

Mother's Day

親愛的媽媽節快樂

除廣為人知的康乃馨外，
在其他國家也會使用
石竹花、玫瑰、茉莉、菊花等，
表達對母親的感謝。

Thank you, Mom!

แม่, ขอบคุณ!

媽媽，
謝謝您！

お母さん，ありがとう！

Gracias, mamá!

엄마, 고마워요！