Institute for Information Industry

資安產業篇

資安防禦 3T融合資安架構 建構數位信任生態治理

在地檢測 制定晶片安全標準 引領產業接軌國際前行

供應鏈資安 資策會推動CMMC生態系 迎戰2026美國國防供應鏈商機

3T融合資安架構
建構數位信任生態治理

> 網路邊界消失，資安問題愈形複雜，當IT x OT x CT沒有邊界時，整合型的3T融合資安架構才能以更全面的角度偵防，打造零信任的數位環境。

數位化時代來臨，企業勢必面臨數位轉型，當場域與裝置大量聯網，企業的營運環境更易遭受資安威脅，急需全新的資安整合解方。為協助廠商數位轉型，資策會推出全新的3T融合資安框架，倡議在網路沒有邊界的情況下，應當整合資訊科技（IT）、運營技術（OT）、通訊科技（CT）等不同領域的資安技術、情資、檢測及人才需求，協助廠商超前部署，因應全新的資安挑戰，提升臺灣產業的數位韌性。

5G、AI、物聯網時代來臨，資安防禦也面臨新型態的威脅。以往強調封閉式的OT管理，講求產線不停機、可用性最大化，在物聯網的興起下，工控系統也開始採取開放與通用性架構，廠房設備對內或對外可透過5G、WiFi、藍芽等通訊協定溝通，讓場域內部容易遭受木馬、病毒等威脅。尤其在5G的開放架構之下，裝置與裝置之間，甚至企業廠房與外部間的場域都會透過CT相互鏈結，不只外部網路環境容易出現安全性弱點，內部工控與IT系統也會因萬物聯網而門戶洞開，讓資安防護更加困難。

當網路的邊界消失，資安不能再靠孤島式或護城河式的單一防火牆來進行防禦，尤其未來IT將逐漸與OT整合，網路通訊解決方案也將朝向6G、低軌衛星等高頻寬、高覆蓋率的混合式網路發展，企業的防禦工具更應該要與時俱進，從全域通訊的角度來超前部署。

為因應無所不在的資安威脅，資策會針對IT x OT x CT等不同領域提出3T融合的資安架構，打造可靠穩定的企業資安聯防機制，並為企業關注的外在威脅、內部風險與法律合規等問題提供解方。例如，IT領域注重機密性、資料保護等需求，資策會運用AI及情資偵防技術整合，主動剖繪駭客攻擊軌跡、病毒碼分析比對，以及威脅行為軌跡推估，打造一站式「Ransom Hunter勒索軟體智能獵捕平台」，建立零勒索的雲端服務環境，保護企業的珍貴數位資產。

製造業場域若發生工安事件，輕則產線停擺，重則造成人命傷亡，因此工控設備需要更加嚴密的資安防護措施。針對具有特殊工控協議，產線需穩定持續運行的工控設備或智慧製造場域，資策會提出包含資安健診、長期監控、設備框架演練及數位分身攻擊探析技術的ICTD（Industrial Cyber Threat Detector，工業控制資安威脅偵測系統）偵防檢測工具，可有效及早預防察覺OT的網路潛伏攻擊，令產線能穩定運行，管理者能方便管理營運，維護場域資訊安全。

針對電商平台詐騙案層出不窮，資策會研發出防詐雷達，化被動為主動，將事後通報模式改為事前聯防，每日掃描露天與蝦皮平台上超過40萬件商品，以AI信賴風險預警模型辨識高風險產品，一但出現疑慮商品，即通報電商平台，再以人工複查，降低消費者受害風險。

網路無國界，資安的問題風雲詭譎，當網路架構越來越沒有邊界，企業更須重視資安的事前偵防與檢測，防患於未然。資策會基於3T融合所研發之自主核心技術，以多層次的逐步整合與防禦，提供產業界彈性的資安防護機制，解決IT x OT x CT邊界消失衍生的資安問題，守護企業重要的機敏資料與設備，因應越來越嚴峻的資安挑戰。同時，該核心技術可透過技轉賦能廠商，提供廠商進一步開發產品，掌握3T領域商機，健全臺灣的產業資安體系，提升我國資安防護能量。

IT偵防
勒索病毒不上門

RansomHunter
勒索軟體智能獵捕平台

駭客無所遁形！
以AI智能輔助企業建立
全方位資安偵防技術

OT健檢
產線資料不外洩

ICSentry
工控資安威脅分析平台

提升生產線安全
傳統產線也能放心智能化

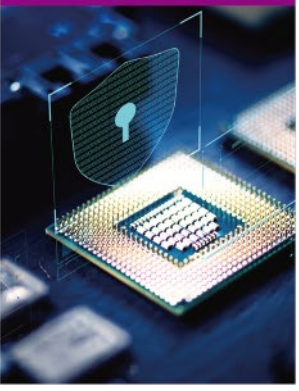
CT檢測
5G合規韌性加倍

5GSec Assure
5G資安自動化檢測平台

5G設備資安預檢測
建立第一道風險防線

制定晶片安全標準
引領產業接軌國際前行

臺灣爲全球半導體重鎮，有完整上、下游供應鏈。爲強化臺灣晶片安全檢測能量，鞏固半導體供應鏈資安及韌性，全臺第一間晶片安全聯合檢測實驗室集結產官學研聚焦晶片安全議題，制定產業標準，開發檢測工具並力推接軌國際，提升我國產業競爭力。



臺灣具有半導體先進製程與完整的產業供應鏈，晶圓製造、IC封測市占世界第一，從手機、筆電、電動汽車到智慧穿戴，都可看見臺灣晶片的蹤影。近年由於晶片資安漏洞與地緣政治牽動半導體供應鏈，如何確保臺灣所提供之晶片產品符合國際標準，獲得全球供應鏈廠商的信賴，成為我國資通訊安全的重要議題。

資策會所成立的全臺第一間晶片安全聯合檢測實驗室，率先制定我國首份晶片安全標準暨測試規範，並經台灣區電機電子工業同業公會（TEEMA）發布成為產業標準，不只為我國半導體產業建立晶片安全遵循指標，也可帶動國內實驗室投入人才培育，擴散硬體晶片安全檢測技術至產業，強化我國晶片安全檢測能量。

臺灣半導體在全球具有重要領先地位，資策會以第三方協力機構角色，整合產官學研能量，攜手SGS Brightsight、鑑智實相、閎康科技、國立中興大學、國立成功大學等機構策略同盟，成立晶片安全聯合檢測實驗室，為臺灣業者提供符合國際標準認證之晶片檢測服務，使我國業者不用遠赴海外，即可在國內就近檢測，取得正規且受國際認可的測試結果，大幅降低產品開發時程與送測成本，有助業者推動外銷，並提升整體競爭力。

由於資通訊產品在整個產品生命週期階段皆可能受到資訊安全攻擊，隨著網路威脅日趨嚴峻，不只軟體、韌體易受到攻擊，近年包括硬體也成為網路攻擊目標。而一份資通訊最終產品可能包含來自不同供應商之元件，若於半導體製程中沒有檢測出安全漏洞，容易對晶片及最終產品產生資安威脅。

01

資策會資安所

銜接政府能量、制定資安標準及測試規範經驗、物聯網設備檢測技術、熟悉臺灣本土市場

02

SGS Brightsight

晶片安全檢測經驗、研發專業檢測儀器、熟悉國際精片安全相關法規及標準

03

國立中興大學

硬體木馬攻防、旁通道攻擊研究與實作、晶圓缺陷檢測自動化

04

國立成功大學

加密電路之掃描鏈及國際測試標準電路攻防、超大型積體電路設計與測試

因此，資策會利用自主研發技術完成晶片旁通道攻擊檢測，及硬體木馬惡意威脅檢測等工具，可及早找出潛在資安威脅，而我國晶片安全標準採納硬體木馬檢測，標準更是高於國際規範，國內業者若通過實驗室檢測，意味著產品更加可靠安全，更容易被納入採購供應鏈。

為提升臺灣對晶片安全的重視，並力促我國晶片檢測標準能與國際對接，資策會與國際標準組織GlobalPlatform（GP）簽署MOU，共同參與標準制定，彼此積極合作，期盼能共同推動IoT平台安全評估標準SESIP的相關合作，未來達到彼此標準互認，落實「在地檢測、全球通行」的目標。此舉可減少廠商國外送測時間與成本，並提升我國晶片產品在物聯網安全和驗證生態系統的國際形象。

過去我國實驗室多著重於軟體資安防護，硬體晶片的資安防護雖有豐富研究能量，但檢測技術尚未落實於場域。資策會成立晶片安全聯合檢測實驗室，則以自主技術研發為基礎出發，協助業者從產製源頭即注入資安思維，並輔導業者儘早通過國際資安標準規範，提升臺灣IC產業晶片安全。

除成立國際認可之晶片安全聯合檢測實驗室，資策會並於各大專院校舉辦晶片人才培訓講座，培育硬體晶片資安人才，未來並將持續與策略夥伴合作，發揮加乘優勢，以「在地檢測，全球通行」為目標，強化我國硬體資安技術，擴大晶片的安全檢測能量，期盼早日活絡資安產業，建構我國晶片的安全生態系。

資策會推動CMMC生態系

迎戰2026美國國防供應鏈商機

美國國防部預計2026年實施「資通安全成熟度模型驗證」（CMMC 2.0）做爲國防採購合約的驗證基準，全面促進30萬家廠商落實供應鏈安全。爲協助臺灣產業儘速接軌CMMC合規，掌握進入國際市場的契機，資策會著手研究CMMC規範，從人才培訓開始，到廠商合規輔導、籌備在地驗證單位等，一同與產業打造CMMC生態系。

為確保國家機密資訊安全，防止機敏資料外洩，2020年美國國防部針對採購供應鏈推出「資通安全成熟度模型驗證」（Cybersecurity Maturity Mode Certification, CMMC）框架，要求承包商應依據專案資訊之機敏性而具備相對應等級的網路安全資安成熟度，並於隔年推出CMMC 2.0版本（目前處於立法階段），提供各級承包商遵循，預計2026年全面實施。

CMMC是以NIST SP 800-171為基礎的資通安全成熟度模型機制，主要保護聯邦合約資訊（FCI）以及受控非機敏資訊（CUI），共分基礎防護級、進階防護級及專家防護級三個級別，除了扣合國家資安標準、幫助相關廠商提升網路安全與合約資訊的防護能力外，也讓政府機關得以依照安全級別，驗證產業供應鏈的資安防護情況。

CMMC實施後，屆時要參與美國國防部供應鏈的廠商，皆須取得CMMC驗證或自評，才能承攬相關採購合約，預計影響全球30萬家廠商、約8,400億美元商機。未來CMMC也將成為具有指標性的供應鏈資安規範，並受到業界擴大採用，成為其他領域供應鏈資安規範的借鏡。

資策會身為我國推動CMMC計畫的主要執行單位，為協助臺灣產業符合CMMC合規要求，搶攻美國國防產業的商機大餅，自2022年起投入CMMC相關規範及生態環境的研究，並與美方緊密合作以獲取第一手資訊，透過三大面向協助產業提早因應及準備。

資策會除結合相關資源培訓諮詢顧問，也積極透過講座課程、工作坊等方式，為資安、資服及關鍵產業培訓CMMC專業人才，成為未來推動供應鏈資安分級的種子人力，以強化輔導產業導入CMMC的實力。

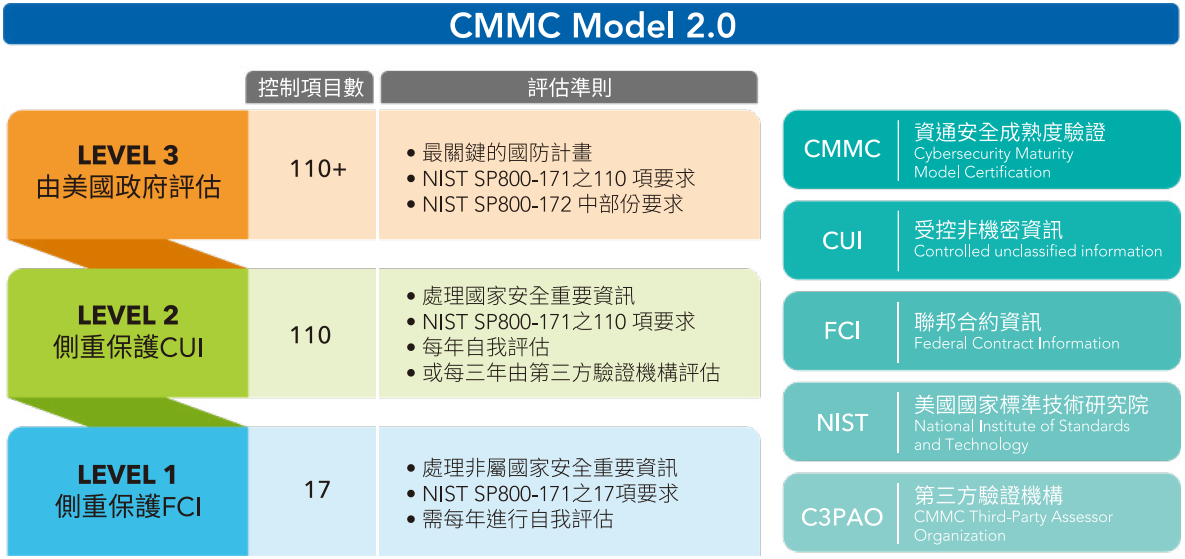
2022年以來資策會積極與美方進行交流，透過交流會議美方分享NIST SP800-171，更特別舉辦工作坊培育臺灣評估員，此為美方首次為非英語系國家提供相關專業培訓，象徵我方資安領域國際合作進一步深化，有助於臺灣提高資安能力，強化兩國互信關係，確保資安標準作業的共識和遵循。

C3PAO目前僅開放美國公司申請，資策會初期以美方NIST SP800-171導入方法與評估經驗，輔導供應鏈廠商優先準備，再逐步建立驗證能量，成立在地C3PAO。

未來待臺灣取得美國授權以後，即能迅速在臺灣建立本地包括諮詢、評估、驗證等的CMMC服務生態系，使我國廠商能就近取得驗證，節省合規時間與成本。

因應地緣政治危機，臺灣資通訊供應鏈在全球具關鍵地位，與軍工相關的航太、半導體、電子、航空造船與機械領域企業，勢將面臨CMMC合規的衝擊。

資策會率先輔導臺灣關鍵廠商與其下游供應商群共同建立NIST SP800-171示範案例，已成功在臺灣國防工業之指標企業及其供應鏈導入CMMC合規作業，成為首個第三方驗證示範場域，象徵臺灣在供應鏈資安上邁入新階段。



新版CMMC 2.0將簡化成3個等級，並依據不同等級制定控制項目及評估準則

財團法人資訊工業策進會
INSTITUTE FOR INFORMATION INDUSTRY

中文官網
Facebook
DxBAR