INSTITUTE FOR
INFORMATION
INDUSTRY

資安產業篇

資安防禦

建構數位信任
資策會力推數位信任永續指數（DTSI）

車載AI

建立資安堡壘
推動車載AI資安檢測及低軌衛星資安防護

iii EVOLUTION
資策會45週年

資安科技研究所

建構數位信任
資策會力推數位信任永續指數（DTSI）

數位經濟蓬勃發展，AI技術驅動產業變革，企業勢將面對更為複雜的網路監管及法遵法規。為此，資策會推動「數位信任永續指數」（DTSI）與CISO Agent，協助企業檢視組織內部的資安成熟度，建立數位信任機制，強化資安量能。

投資市場很常使用指數來評估一個市場或某些領域的企業整體表現，例如反映美國經濟表現的標普500指數，以及反映高科技、IT、生物技術及半導體動態的那斯達克指數等等。而被業界稱為「恐慌指數」的VIX指數，則隱含投資人對美股前景的看法，指數越高，代表對美股的前景越感到不安，反之亦然。

全臺首創「數位信任永續指數」

除了投資型指數，近年ESG議題發燒，著名的道瓊永續指數（Dow Jones Sustainability Index, DJSI）也成為投資者關注的一項指標。2023年，臺灣有35家企業入選道瓊永續指數，橫跨十大產業，這不只代表入選企業對永續發展的投入，也意味著可以吸引投資人的目光，並左右他們的資金決策。

ESG的多項評估與量化指標成為公司治理的重要事項；而攸關資訊安全與隱私保護的數位信任概念，資策會也積極建構一套評鑑標準：「數位信任永續指數」（Digital Trust Sustainability Indexes, DTSI）。DTSI指數是全球首創，也是全臺第一個聚焦於數位信任的指標。如同道瓊永續指數特別關注環境、社會以及公司治理三大面向，DTSI指數從組織治理、產品服務及供應鏈信任等三個面向，從投資角度來評估企業是否具備數位信任的可持續發展能力。

通用型評估標準

目前業界對於資安的合規要求，大多遵循產業資安規範或採取導入ISO 27001等國際資訊安全管理標準認證，但多偏向資訊系統或是網路傳輸的安全性為主；在未來數位經濟環境下，一間企業要提供可信賴且安全可靠的產品或服務時，往往要將數位信任的DNA，整合至業務、產品研發創新、客戶服務及管理階層，這時就需要更為廣泛的通用型指標。

DTSI指數的框架與評估機制，以數位信任為發展核心，用意在彰顯企業隱性的信任價值與永續經營的量能。指數設計的方向，從企業的組織治理、產品服務到供應鏈信任等等，都是關注的面向，因此DTSI指數關心的不只是企業的IT技術是否到位，資訊安全管理是否合規，導入AI應用前的數據、資料管理、與上下游的供應鏈信任等，能否建立由內而外、從組織到合作伙伴的安全能力，也被納入到指數的評估項目之中。

因為DTSI指數廣泛檢視企業的數位信任能力，從指數的評估項目，也可回頭檢視企業的資安治理現況，以及在數位信任的發展程度，例如，在資安治理評估項目當中，會同步檢視企業處理「資料、個資、隱私治理」、「AI資安」等議題；在產品服務評估項目中，將檢視資通類產品的檢測情況；在供應鏈信任中，也納入「安全一致性」、「產業聯防」等評估項目。DTSI指數會一一檢視企業內部不同的評估項目，予以評分及加總，再得出總分，顯示企業在數位信任永續方面的表現。

為企業資安做體檢

由於DTSI指數的評估對象涵蓋不同產業及不同規模企業，每間企業所面臨的經營環境與產業成熟度不同，DTSI指數會逐一調整評估項目的加權比重，真實反映產業的現況。比如在高科技產業，要求資料全部透明恐

有執行難度，資料透明度的權重會因應下調；保險金融業因應監管需求，資料管控的權重就會調高。此外，資策會在設計評估項目時，也與業界密切交流，傾聽企業、產業公協會及具公信力法人代表的建議，讓設計出來的評估項目更具公信力。

對企業而言，參與DTSI指數的評比就像參與一場馬拉松比賽，透過指數中的評比項目，一一檢視參賽選手（企業）的體能、技術水準與耐力，進而激勵組織進行調整，此舉不但能提升企業形象，也能強化企業內部的風險管理，並促進企業創新，促使企業高階主管以更系統化的方式來建構企業的數位信任，強化資安能力。當企業的數位透明度提升，消費者及投資者會更對企業更有信心，提升整體的企業競爭力。

維運管理解方，解決資安痛點

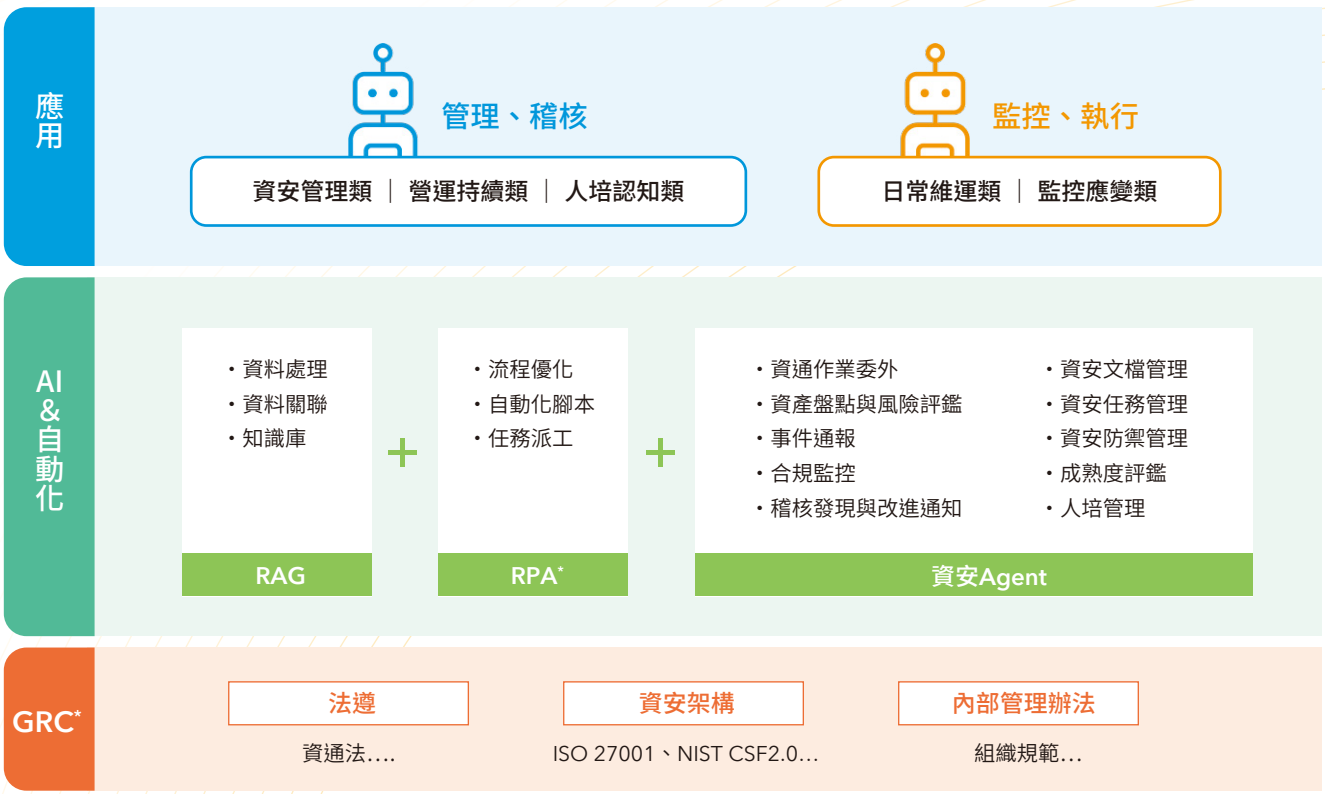
企業投入數位轉型的同時，也面對越來越多的資安合規要求，新興科技的快速發展，更對資安管理工作帶來挑戰。資策會在建構DTSI指數之際，亦從產業執行資安工作的痛點著手，以AI應用為基礎開發各種資安Agent，希望透過「CISO Agent」服務來協助企業資安長全方位檢視、落實資安管理及維運事項，並據此評鑑資安成熟度的實施成果，此工具可進行資安風險管理，也有助於企業符合DTSI指數的標準。

資策會「CISO Agent」內設計多款協助資安長管理的資安Agent軟體工具，包括資通作業委外採購合規小幫手、法遵合規監控模組、資安事件通報等，例如，有採購需求的同仁，可用自然語言與小幫手進行對話，詢問資通委外作業需準備哪些資安文件與注意事項，採購流程的履約、驗收及維運過程中需要的資安清單也會一一列好，彷彿採購人員的貼身秘書一樣細心。

「CISO Agent」運用AIGC技術賦能業界資安量能，主要解決企業內部人員資安認知、法規不熟與人才不足問題，提升內部資安管理效率，能進一步協助落實資安成熟度評鑑與治理機制，減輕負擔外，亦能促進產業資安聯防。

事半功倍，有好的工具強化產業的資安量能，資策會以核心技術賦能資服業者，提供經過實證並精進的資安治理工具，共同協助企業的數位轉型之路，可以越走越遠。

CISO Agent



* RPA: Robotic Process Automation
GRC: Governance, Risk, and Compliance

CISO Agent協助企業落實資安政策與管理

資安科技研究所

建立資安堡壘
推動車載AI資安檢測及低軌衛星資安防護

下一代的通訊發展結合AI人工智慧，不管是地面奔馳的智慧車，還是連到天上的低軌衛星，都存在著資安防護的重要議題。資策會以自有技術研發接軌國際資安防護標準，找出系統漏洞與安全性弱點，並將技術賦能資安業者及檢測實驗室，打造出基磐穩固的數位信賴產業。

駕駛坐進電動車中，手握方向盤，控制著智慧駕駛輔助系統，充滿科技感的儀表板顯示即時車況，車上的科技配備也正在為駕駛分憂解勞。敏銳的雷達感測或AI影像辨識偵測到前方人車或障礙物，智慧化的自駕系統自動跟車、緊急剎停、汽車防撞，提醒左右來車，以各種先進的數位技術，提前預防事故發生，防患於未然。

在路上奔馳的電動車越來越智慧化，引進生成式AI、5G、雷達偵測及先進駕駛輔助系統（ADAS, Advanced Driver Assistance Systems）等主動式輔助科技，讓電動車的行車更安全。不過，伴隨電動車的技術演進，為了要解放駕駛的雙手，智慧車載系統越來越主導車輛的操控，車上的自駕系統也仰

賴智慧運算來介入駕駛的行為。一旦電動車行駛在馬路上，攸關行車安全的車載AI系統是否安全，就連國際大廠也無法輕忽。與此同時，隨著衛星通訊技術的商業化，車載衛星系統（Vehicular Satellite Communication Systems）可為地面車輛網路提供有效且快速的服務，是推動智慧交通系統的關鍵要素。

檢測工具強化車載資安能力

車載AI系統出包影響廣泛，攸關到乘車安全、隱私保護及產業競爭力，如把錯誤的資訊不斷拋去訓練車上的AI模型，經過千百次以上的訓練後，車載系統有可能把綠燈識別為「停止」，把紅燈識別為「繼續前進」，如此將天下大亂。

因此，由資策會自主研發車載AI資安的檢測工具，研究並對照現行的國際資安框架、產業標準及網路安全弱點，建立指引與檢測工具，攜手國內的檢測單位與驗證實驗室，期能協助供應鏈車廠通過國際資安合規，增強車載資安的能力。

打造完整車載AI資安生態系

目前市面上的車載AI系統包括可對外辨識行人及號誌的「駕駛輔助系統ADAS」，可對內監控是否有疲勞駕駛的「駕駛監控系統DMS」，及車載中的語音控制及大型語言模型（LLM, Large Language Model）系統，資策會將從中選擇重要項目來開發檢測工具，並開發擬真攻擊腳本，模擬AI的資安攻擊情境。

外部惡意攻擊AI的情境，如同小偷闖空門或破窗而入，駭客可利用後門長驅直入，在系統裡「翻箱倒櫃」，可能的風險包括竊取AI模型、滲透系統，或是把模型加以竄改。如不預先檢測AI系統上潛在的安全漏洞，駭客甚至可能駭入AI系統，造成重大的安全事故。

鑑於廠商不易理解複雜的AI原理及應用情境，加上國際還未有統一的車載AI資安標準，對於廠商要達到合規造成不少門檻，因此，資策會預計於2024年Q4推出相關的資安檢測指引，希望結盟產業公協會與車用資安業者，共同協助廠商檢測車輛的整個生產環節是否合規，接軌國際規範，拓展車用產業的機會，並打造完整優質的車載AI資安生態系，整體實施策略如下頁圖示。

低軌衛星資安成下一波攻防重點

與通訊協定相關的另一資安議題是低軌衛星。近年低軌衛星因為戰爭題材而浮上檯面，進而引爆下一波產業革命的熱門話題。低軌衛星可以做到高覆蓋率及高頻寬率，研發成本低，升空容易，又不易受到地面嚴苛地形與氣候的影響，在建立韌性通訊、國防自主、應變重大天災與應對戰爭等議題上，更突顯出低軌衛星的競爭優勢。

在疫情前，全球衛星大約近4,000顆，至2023年底，已經爆發式成長到9,000顆。不過短短4年，國際間的衛星數量已經翻倍。隨著衛星產業蓬勃發展，伴隨的資安攻擊也開始引起市場的關注。目前全球已發生數起與衛星有關的資安攻擊事件，駭客曾利用管理站韌體更新攻擊，造成數據機離線，使衛星無法連線；也曾經攻擊地面控制中心，讓衛星網路供應商的客戶面臨通訊中斷的風險。

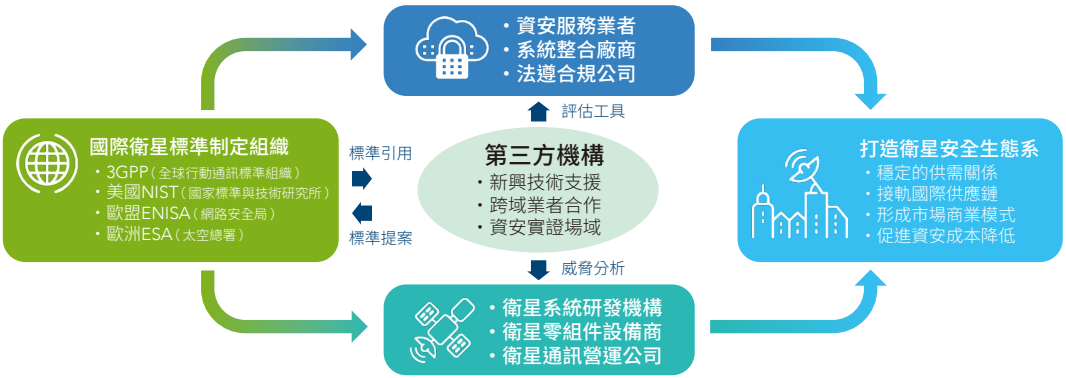
過去太空衛星產業因成本高昂，各國政府機構及商用業者在天上運行的衛星星鏈，都依靠自己的通訊協定形成封閉系統，衛星營運業者資安防護意識較為薄弱，但是當低軌衛星越來越密集，服務覆蓋範圍越來越廣，衛星資安將會牽一髮而動全身，若遭遇駭客攻擊而發生通訊中斷，依賴衛星運作的許多服務將會受到衝擊。

打造具韌性且可信賴的數位產業

資策會注意到衛星與地面終端設備之間通訊潛在的資安問題，因而參考美國國家標準與技術研究所於2023年發布「NIST.IR.8270 Introduction to Cybersecurity for Commercial Satellite Operations（商業衛星運營網路安全指引）」，以國際共通資安標準框架，探討商業衛星產業的網路安全風險管理作法，積極開發低軌衛星的資安評估工具，將衛星元件、通訊元件的軟硬體安全性，都納入衛星資安評估的一環。首先聚焦車載衛星系統安全性整備，希望藉由事前的資安評估，協助衛星系統的開發廠商在設計或開發階段，納入資訊安全的考量，將風險降到最低，並強化資安的防護。

資策會進一步著手研析衛星模擬運行時的攻擊情境，找出可能威脅衛星安全營運的攻擊模式，包括DDoS攻擊（Distributed Denial-of-Service Attack，分散式阻斷服務攻擊）、攔截訊號、資料竊取、資料竄改、上傳偽資訊等，參照國際標準，在實驗室建模及開發腳本，分析駭客的攻擊手法，找出資安漏洞，亦發現偽地面站、資料攔截等駭客攻擊手法，的確會對較少設防的衛星系統造成影響，後續將自研產出之系統弱點擴增於低軌衛星的資安評估工具，並將研究發現與國內業者合作參與3GPP NTN（Non-Terrestrial Networks，非地面網路）安全議題研究及標準提案，為正在制定一致性的衛星國際通訊標準，盡一份心力。

資策會身為第三方公正驗證機構，透過衛星模擬環境威脅建模、腳本演練來對衛星的韌性進行評估，期盼攜手廠商並結合公協會及產業聯盟，一起強化臺灣衛星通訊的網路韌性，不只支持我國資安防護自主研發的能力，也希望能運用自有技術來深耕產業，為低軌衛星資安實驗共創場域，並確保臺灣通訊產業的資安韌性，打造出可信賴的數位產業。



協助產業打造低軌衛星安全生態系

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

中文官網 Facebook DxBAR