Your Gateway to Strategic Insights.

產業研究報告

2026-2027 年台灣製造業雲端服務與資安支出調查

前言

隨著製造業深化數位應用，雲端服務與資通安全成為重要投資課題。本報告依據 2026 年台灣製造業資訊科技投資與應用調查，以 200 家經常雇用員工數 100 人以上的受訪企業為分析基礎，探討傳統與高科技製造業的雲端及資安支出與應用意向，涵蓋 2026 年全年支出估計及 2027 年支出預估，供資服與軟體業者掌握需求。

劉佳芊

Document Code: CDOC20261020004
Publication Date: Oct 2026

Check out MIC on the Internet!
https://mic.iii.org.tw/aisp

目錄

雲端服務支出情形 1
雲端服務應用展望 3
資通安全支出情形 8
資通安全應用展望 11
結論 14
附錄 15

©2026 Market Intelligence & Consulting Institute
CDOC20261020004

圖目錄

圖一、2026-2027 年台灣製造業各項資訊科技平均支出預估及 2027 年成長率 1
圖二、2026-2027 年台灣製造業在雲端服務平均支出預估及 2027 年成長率 2
圖三、2027 年台灣製造業雲端服務支出變動預估 3
圖四、2026-2027 年台灣製造業資訊系統部署方式比重 4
圖五、2026 年台灣製造業預計持續使用或新增導入的雲端服務項目 5
圖六、2026-2027 年台灣製造業預計優先採用 SaaS 形式的資訊系統 6
圖七、2026-2027 年台灣製造業預計增加支出的雲端服務項目 7
圖八、2026-2027 年台灣製造業在資通安全平均支出預估及 2027 年成長率 8
圖九、2027 年台灣製造業資通安全支出變動預估 9
圖十、2026 年台灣製造業資通安全支出變動的主要影響因素 10
圖十一、2026 年台灣製造業資安長或資安官設置情形 11
圖十二、2026 年台灣整體製造業各項資通安全應用與服務導入情形 12
圖十三、2026-2027 年台灣製造業預計持續使用或擴大採用的資安服務與技術 13

©2026 Market Intelligence & Consulting Institute

表目錄

表一、整體有效樣本特性分析 15
表二、有效樣本特性 16
表三、資安服務類型說明 17

©2026 Market Intelligence & Consulting Institute

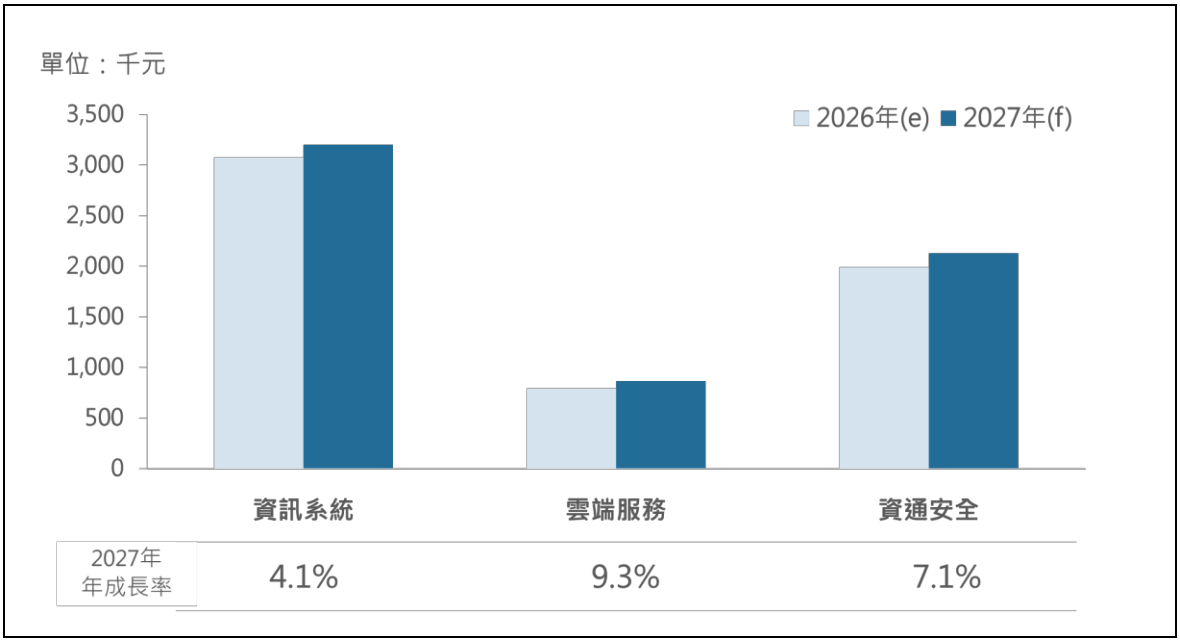
雲端服務支出情形

整體分析：雲端支出增幅居首，資安新增金額較高

整體受訪製造業者 2027 年「雲端服務」平均支出預估成長 9.3%，高於「資通安全」的 7.1%與「資訊系統」的 4.1%，為本報告比較的三項資訊科技支出中，預估增幅最高者（參見圖一）。

然而，「資訊系統」與「資通安全」的平均支出規模仍高於雲端服務，且資安平均支出的預估增加金額在三者中最高。這顯示受訪製造業者在擴大雲端應用的同時，既有系統運作與安全防護仍是重要的投資項目。

圖一、2026-2027 年台灣製造業各項資訊科技平均支出預估及 2027 年成長率



備註：整體製造業 n=200，平均支出計算包含零支出企業；2027 年成長率以 2027 年平均支出相較 2026 年平均支出的變動幅度計算

資料來源：MIC，2026 年 10 月

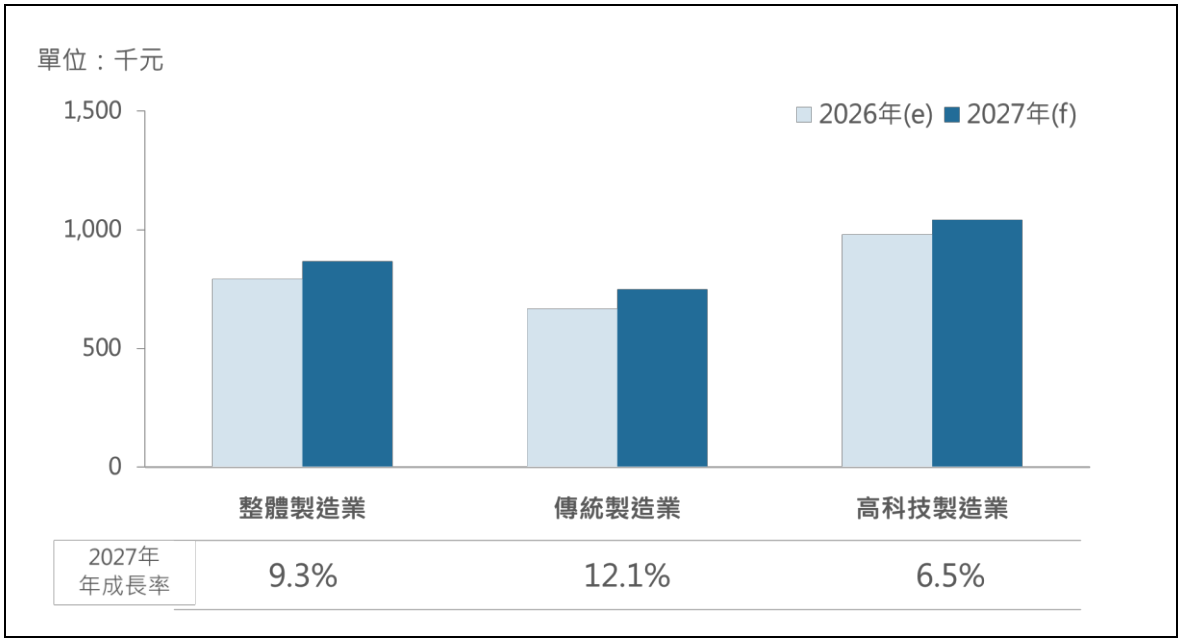
次產業分析：傳統製造支出增幅較高，高科技投入規模較大

產業別方面，傳統製造業 2027 年雲端服務平均支出預估成長 12.1%，高於高科技製造業的 6.5%（參見圖二）。高科技製造業的平均雲端支出規模較大，傳統製造業則

©2026 Market Intelligence & Consulting Institute

呈現較低支出基期與較高預估成長率，顯示兩類受訪企業在投入規模與成長幅度上有所差異。

圖二、2026-2027 年台灣製造業在雲端服務平均支出預估及 2027 年成長率



註 1：整體製造業 n=200，傳統製造業 n=120，高科技製造業 n=80

註 2：平均支出計算包含零支出企業；2027 年成長率以 2027 年平均支出相較 2026 年平均支出的變動幅度計算

資料來源：MIC，2026 年 10 月

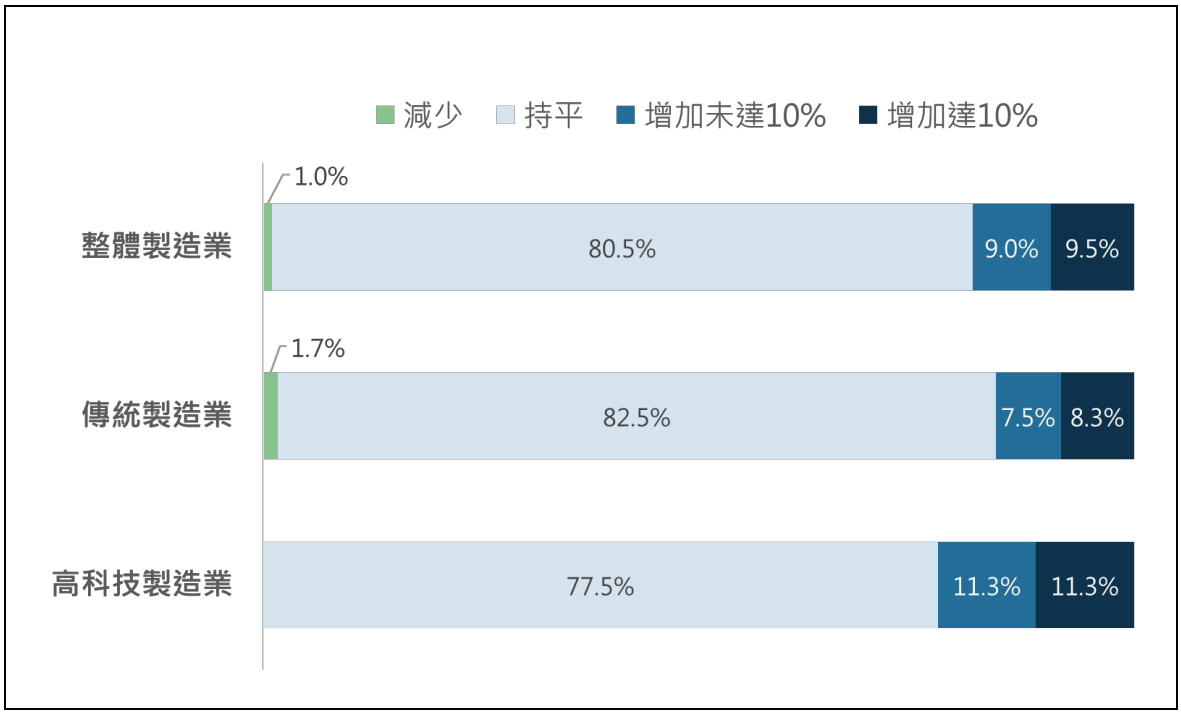
預算變動：雲端支出多數持平，增支企業比重相對有限

雲端服務預算變動方面，2027 年受訪企業中，預計增加雲端服務預算者占 18.5%，持平者占 80.5%，減少者占 1.0%，多數業者預估維持既有預算規模。企業提出的增支原因涵蓋業務擴張、AI 應用、雲端備份及供應商調價，顯示新增支出既包含應用範圍擴大，也涉及既有服務成本上升。

次產業方面，傳統製造業預計增加雲端預算的企業占 15.8%，低於高科技製造業的 22.5%(參見圖三)。傳統製造業呈現平均支出增幅較高、增支企業比重較低的組合；高科技製造業則有較高比重的企業規劃增加預算。此結果顯示，兩類受訪企業的支出成長幅度與增支普及程度有所不同。

©2026 Market Intelligence & Consulting Institute

圖三、2027 年台灣製造業雲端服務支出變動預估



註 1：整體製造業 n=200，傳統製造業 n=120，高科技製造業 n=80

註 2：百分比四捨五入至小數點後一位，合計可能不等於 100%

資料來源：MIC，2026 年 10 月

雲端服務應用展望

部署模式：地端架構比重超過八成，系統上雲採漸進式調整

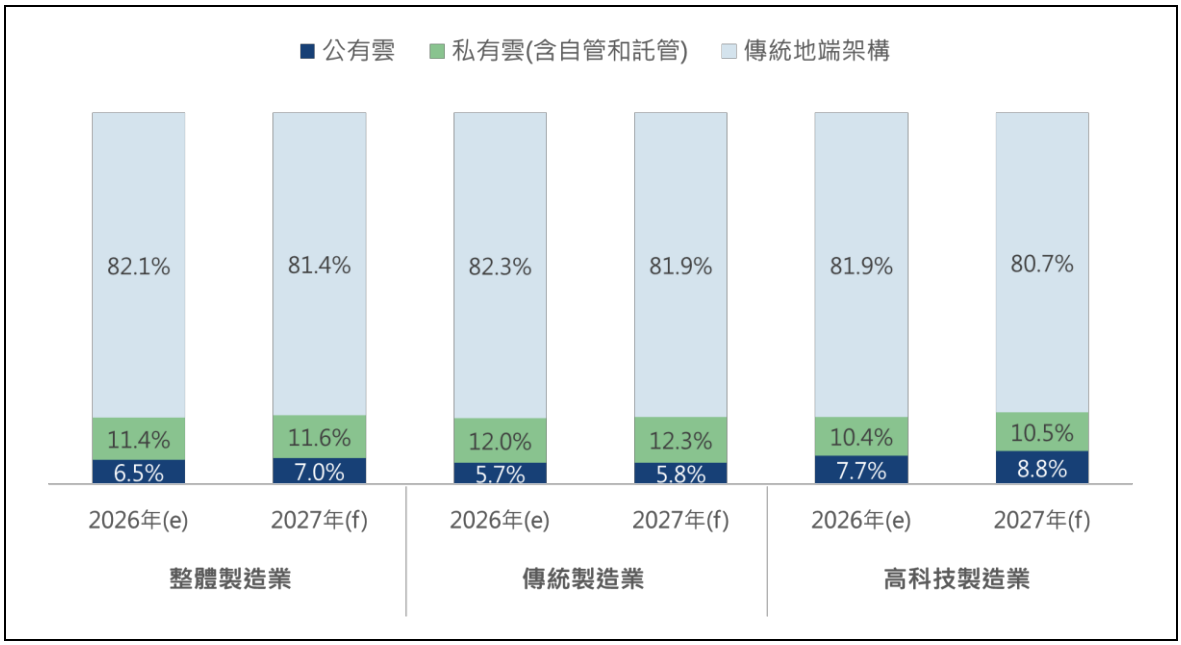
受訪業者資訊系統採用「傳統地端架構」的平均配置比重，從 2026 年的 82.1%預估降至 2027 年的 81.4%；「公有雲」從 6.5%上升至 7.0%，「私有雲」則從 11.4%上升至 11.6%。

兩年度的地端部署比重皆超過八成，且預估變動幅度有限，顯示受訪企業在本次調查涵蓋期間，仍以既有地端架構為主要配置。

次產業方面，高科技製造業「公有雲」部署比重從 7.7%升至 8.8%，傳統製造業則從 5.7%微升至 5.8%；傳統製造業的「私有雲」比重仍較高。反映此二產業的雲端部署選擇有所差異，高科技製造業增加公有雲配置較為明顯，傳統製造業則維持較高的私有雲比重（參見圖四）。

©2026 Market Intelligence & Consulting Institute

圖四、2026-2027 年台灣製造業資訊系統部署方式比重



註 1：此題為受訪業者分別估計 2026 年及預測 2027 年其資訊系統採用公有雲、私有雲（含自管及託管）與傳統地端架構的比重，比重合計為 100%；此為各企業配置比重之平均

註 2：整體製造業 n=200，傳統製造業 n=120，高科技製造業 n=80

資料來源：MIC，2026 年 10 月

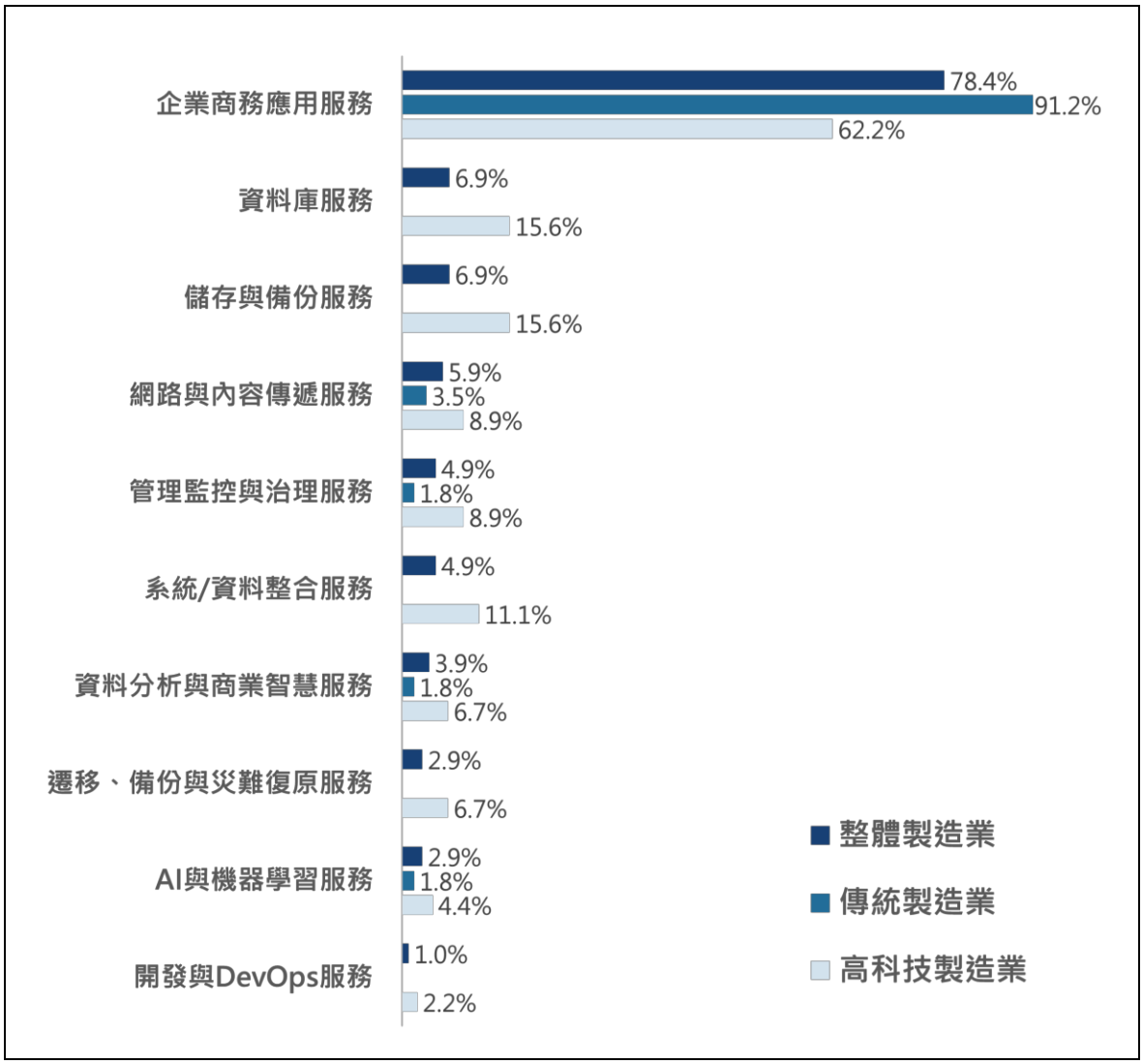
使用情形：需求集中於企業商務應用，高科技服務組合較廣

在 2026 年或 2027 年資訊系統配置包含公有雲或私有雲的 102 家受訪業者中，78.4% 預計於 2026 年底持續使用或新增導入「企業商務應用服務」；「資料庫服務」與「儲存備份服務」各占 6.9%；「網路與內容傳遞服務」及「系統與資料整合服務」則分別占 5.9%及 4.9%。整體而言，現階段需求以可直接支援業務的應用服務為主，資料處理與開發維運等服務的選擇比率相對較低。

次產業方面，傳統製造業選擇「企業商務應用服務」的比重為 91.2%，高於高科技製造業的 62.2%。高科技製造業在「資料庫服務」與「儲存備份服務」的比重皆為 15.6%，「系統與資料整合服務」亦達 11.1%（參見圖五）。綜上所述，傳統製造業的需求較集中於應用軟體，高科技製造業則另涵蓋資料管理與基礎服務，形成不同的服務組合。

©2026 Market Intelligence & Consulting Institute

圖五、2026 年台灣製造業預計持續使用或新增導入的雲端服務項目



註 1：整體製造業 n=102，傳統製造業 n=57，高科技製造業 n=45；樣本包含 2026 年或 2027 年資訊系統配置採用公有雲或私有雲的企業，排除兩年度均為 100%傳統地端架構者；此為複選題

註 2：傳統製造業部分服務項目無受訪企業勾選（比率為 0%），故圖中未顯示對應橫條

資料來源：MIC，2026 年 10 月

SaaS應用：優先支援營運與客戶管理，次產業需求略有差異

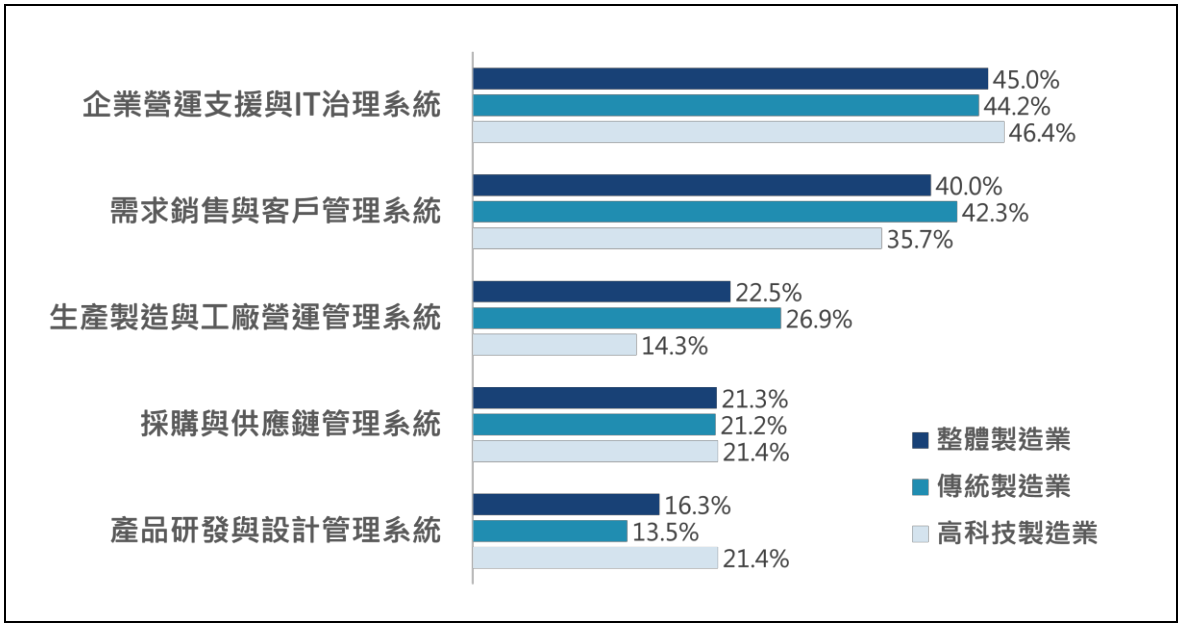
在選擇「企業商務應用服務」的受訪業者中，45.0%於 2026 至 2027 年優先以軟體即服務（SaaS）形式採用「企業營運支援與 IT 治理系統」，40.0%選擇「需求銷售與客戶管理系統」，高於「生產製造與工廠營運管理系統」的 22.5%（參見圖六）。

©2026 Market Intelligence & Consulting Institute

整體而言，受訪企業優先以 SaaS 形式採用的系統，以營運支援與客戶管理居前，生產製造與工廠營運管理的選擇比重相對較低。

次產業方面，傳統與高科技製造業在「營運支援與 IT 治理系統」的比重接近，分別為 44.2%與 46.4%；傳統製造業在「需求銷售與客戶管理系統」的比重為 42.3%，高於高科技製造業的 35.7%。「生產製造與工廠營運管理系統」則分別為 26.9%與 14.3%。傳統製造業的 SaaS 採用意向亦涵蓋工廠營運。資服業者可進一步確認其製造流程、既有系統及資料串接需求，作為方案設計的依據。

圖六、2026-2027 年台灣製造業預計優先採用 SaaS 形式的資訊系統



備註：整體製造業 n=80，傳統製造業 n=52，高科技製造業 n=28；此題樣本為有勾選導入企業商務應用服務（企業應用 SaaS 服務）者；此為複選題

資料來源：MIC，2026 年 10 月

支出意向：AI工具與資料平台居前，跨環境管理亦受關注

在上述 102 家受訪業者中，2026 年至 2027 年預計增加支出的雲端服務項目，以「新興 AI 技術或工具平台(如大語言模型 API、生成式 AI、機器學習營運管理 / MLOps、Agent 建置平台等）」的 37.3%居首，其次為「雲端資料平台」的 33.3%，以及「混合雲 / 多雲管理」的 30.4%。

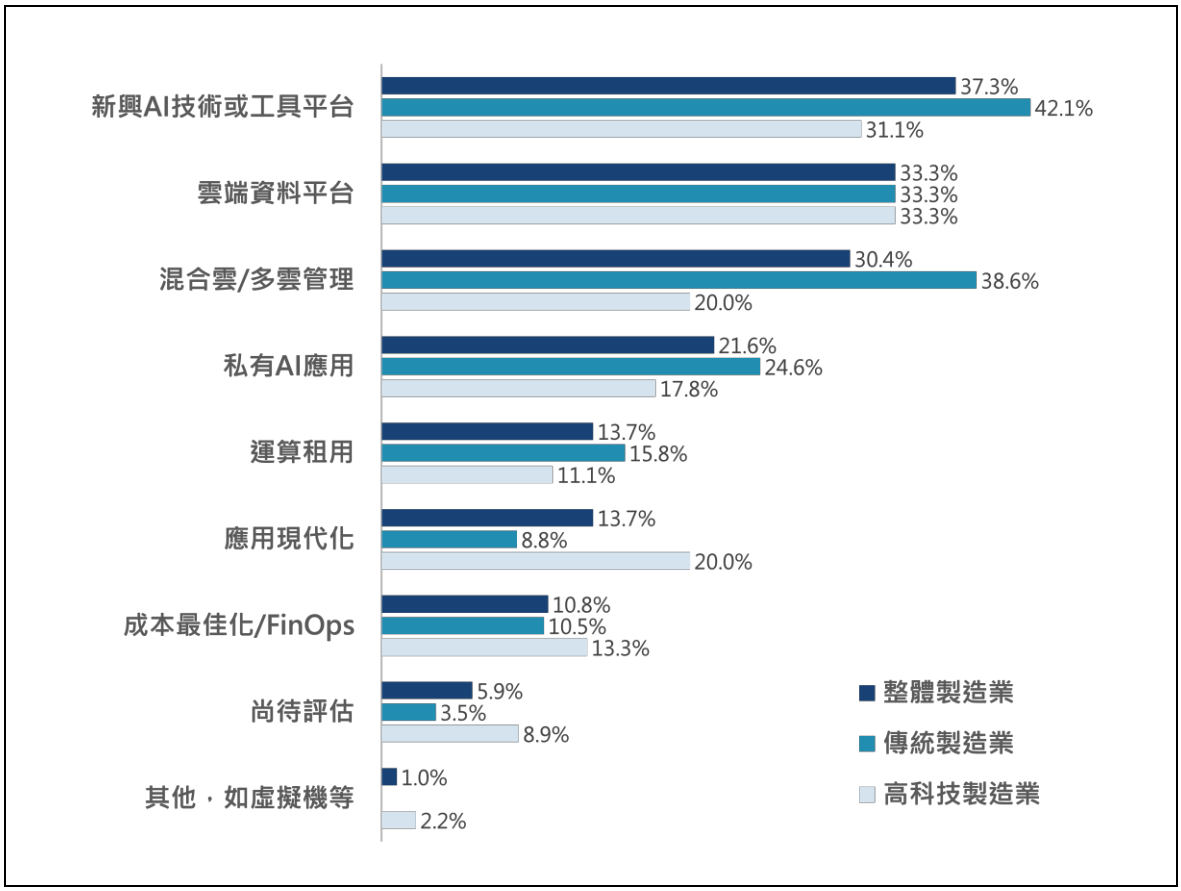
©2026 Market Intelligence & Consulting Institute

「私有 AI 應用（如私有模型推論平台、私有雲等）」與「運算租用（如用於 AI 訓練或推論之 GPU / TPU 算力租用）」則分別為 21.6%與 13.7%。顯示受訪企業的雲端增支意向涵蓋 AI 工具、資料平台及跨環境管理等項目。

次產業方面，傳統製造業在「新興 AI 技術或工具平台」的增支意向為 42.1%，高於高科技製造業的 31.1%；「混合雲 / 多雲管理」分別為 38.6%與 20.0%。「私有 AI 應用」和「運算租用」亦略高於高科技製造業。

高科技製造業在「應用現代化（如容器化應用程式、微服務、無伺服器運算 / Serverless 等）」的選擇比重為 20.0%，高於傳統製造業的 8.8%（參見圖七）。綜合而言，兩類受訪企業的雲端增支項目有所差異，資服業者可據此進一步確認其應用情境與導入條件；惟選擇比重不代表投入金額或應用成熟度。

圖七、2026-2027 年台灣製造業預計增加支出的雲端服務項目



註 1：整體製造業 n=102，傳統製造業 n=57，高科技製造業 n=45；樣本包含 2026 年或 2027 年資訊系統配置採用公有雲或私有雲的企業，排除兩年度均為 100%傳統地端架構者；此為複選題

註 2：傳統製造業部分服務項目無受訪企業勾選（比率為 0%），故圖中未顯示對應橫條

資料來源：MIC，2026 年 10 月

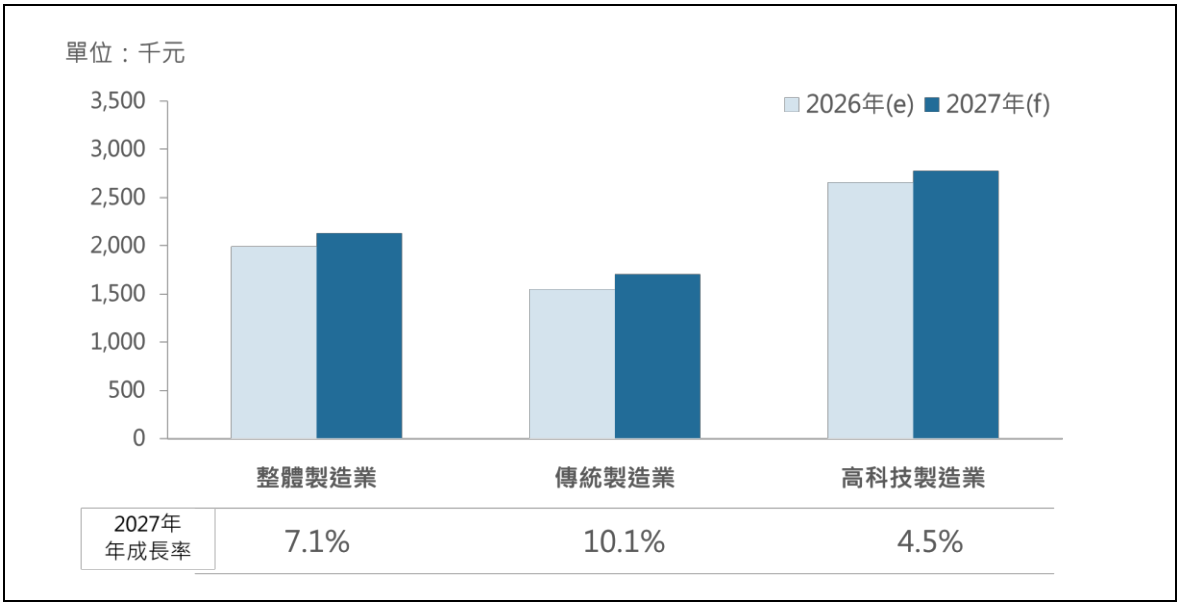
©2026 Market Intelligence & Consulting Institute

資通安全支出情形

整體分析：傳統製造支出增幅較高，高科技投入規模較大

整體受訪業者 2027 年資安平均支出預估成長 7.1%；傳統製造業成長 10.1%，高於高科技製造業的 4.5%，但高科技製造業平均支出規模高於傳統製造業(參見圖八)。

圖八、2026-2027 年台灣製造業在資通安全平均支出預估及 2027 年成長率



註 1： 整體製造業 n=200，傳統製造業 n=120，高科技製造業 n=80

註 2：平均支出計算包含零支出企業；2027 年成長率以 2027 年平均支出相較 2026 年平均支出的變動幅度計算

資料來源：MIC，2026 年 10 月

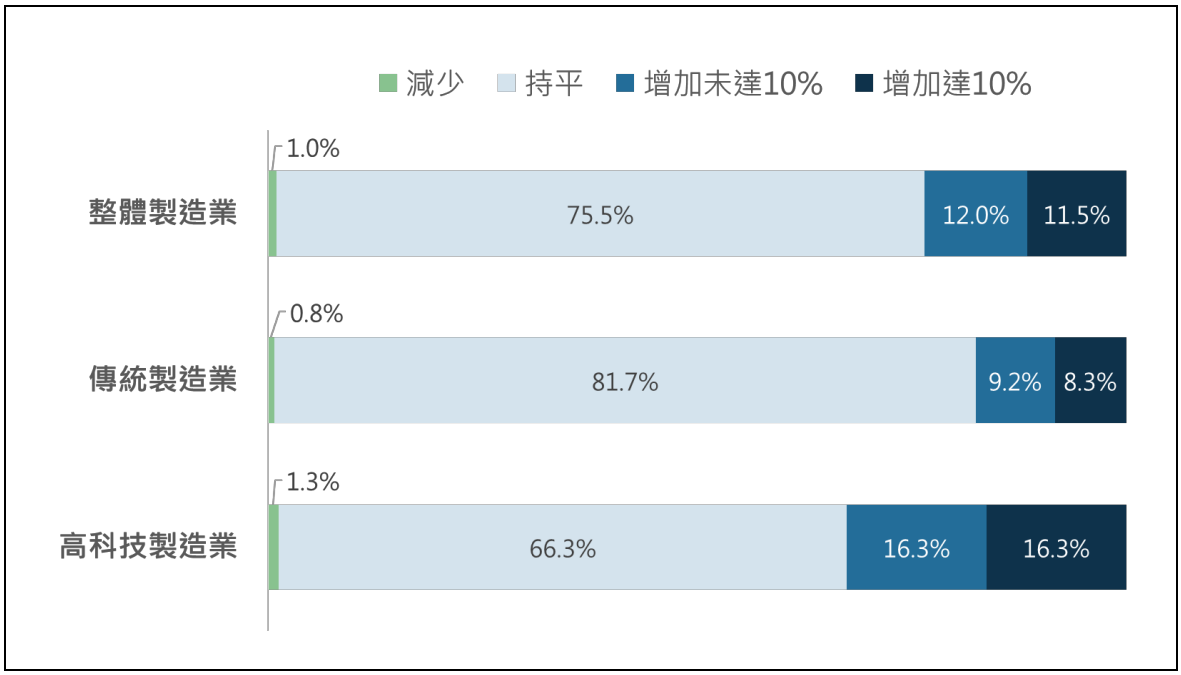
從整體受訪業者 2027 年增支分布來看，75.5%業者預估資安支出持平，23.5%增加，僅 1.0%減少，呈現出 2027 年資安預算規劃以維持既有投入為主，部分企業加碼。

次產業方面，高科技製造業預計會增加資安支出的企業占 32.5%，高於傳統製造業的 17.5%。高科技製造業規劃增支的企業比重較高；傳統製造業則呈現平均支出增幅較高、增支企業比重較低的情形 (參見圖九) 。

進一步觀察業者回覆的增支原因，包含新廠與系統建置、設備汰換、授權續約及費用上漲；部分減支則源於專案完成、設備建置後改付保固費用，或預算與人力縮減。市場需求因此涵蓋新增建置、既有防護更新與後續維運，並隨企業營運及專案進度調整。

©2026 Market Intelligence & Consulting Institute

圖九、2027 年台灣製造業資通安全支出變動預估



註 1：整體製造業 n=200，傳統製造業 n=120，高科技製造業 n=80

註 2：百分比四捨五入至小數點後一位，合計可能不等於 100%

資料來源：MIC，2026 年 10 月

變動因素：合規與威脅考量居前，業務需求亦影響投入

在 2026 年有資安支出的受訪業者中，65.8%將「法規或合規壓力」列為支出變動因素，62.6%選擇「威脅或事件驅動」，均高於「公司策略或業務驅動」的 42.2%。

顯示受訪業者在調整資安預算時，較常將符合外部規範與因應攻擊風險列為主要原因（參見圖十）。因此，資安方案的價值須同時兼顧合規與營運保障，資服業者可結合防護措施、合規查核及風險改善成效，協助企業建立更明確的資安投資依據。

相較之下，人才與組織因素僅占 8.0%，較少被列為支出調整的主要原因。然而此結果僅能反映各項因素在預算決策中的相對優先程度，尚不能據此判斷企業的人才與組織能力是否已足夠。

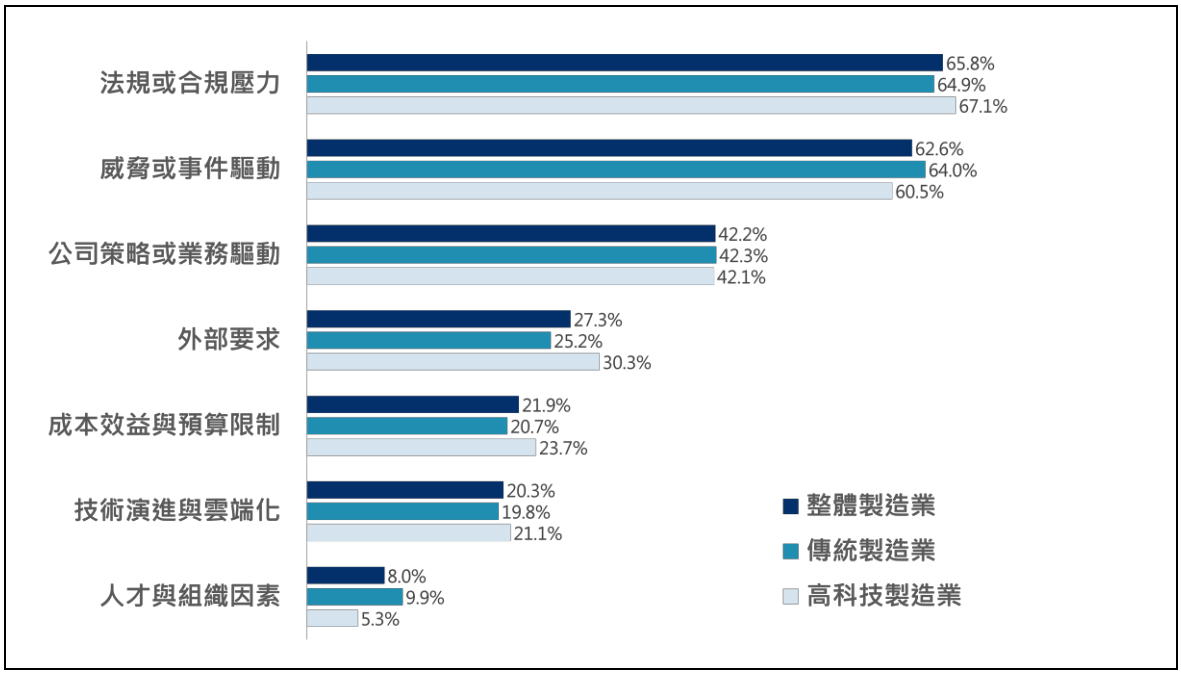
次產業方面，傳統製造業將「威脅或事件」列為支出變動因素的比重為 64.0%，略高於高科技製造業的 60.5%；高科技製造業則在「法規或合規壓力」、「外部要求」的比重較高，分別為 67.1%及 30.3%，傳統製造業為 64.9%及 25.2%。

兩類受訪業者均以合規與威脅為主要考量，各項因素的選擇比重略有差異，尚不足以據此判定兩類產業具有明確不同的預算決策模式。

©2026 Market Intelligence & Consulting Institute

在資安支出變動原因的開放回答中，傳統製造業提及防火牆、端點防護、委外監控、資安管理制度與零信任；高科技製造業則提出端點偵測及回應（Endpoint Detection and Response，簡稱 EDR）、資料防洩漏（Data Loss Prevention，簡稱 DLP）、弱點掃描與入侵偵測委外，以及 ISO 27001 資安管理驗證。上述回覆涵蓋防護工具、專業監控與驗證輔導，反映部分受訪業者的具體投入項目。

圖十、2026 年台灣製造業資通安全支出變動的主要影響因素



備註：整體製造業 n=187，傳統製造業 n=111，高科技製造業 n=76；此題樣本排除 2026 年資安支出金額為零元者；此為複選題，最多 3 項

資料來源：MIC，2026 年 10 月

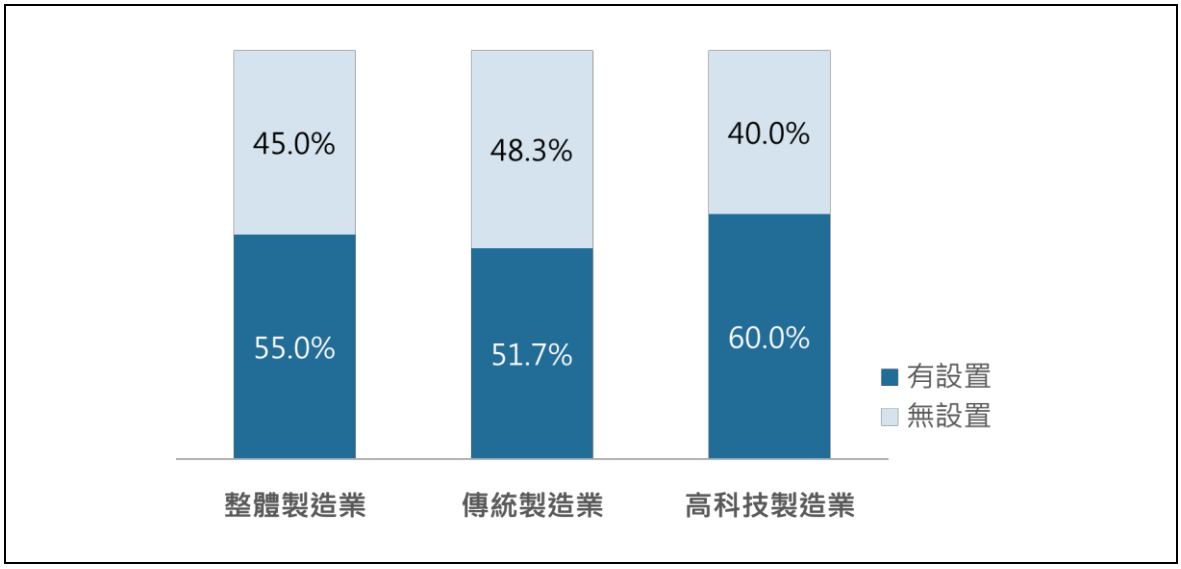
©2026 Market Intelligence & Consulting Institute

資通安全應用展望

治理配置：過半企業設置資安主管，高科技比重較高

受訪業者中有 55.0%已設置資安長或資安官；其中，高科技製造業為 60.0%，高於傳統製造業的 51.7%（參見圖十一）。職位設置反映組織安排，但本調查未進一步確認其專兼任、授權及資源配置，尚不足以判定實際管理成效。

圖十一、2026 年台灣製造業資安長或資安官設置情形



備註：整體製造業 n=200，傳統製造業 n=120，高科技製造業 n=80

資料來源：MIC，2026 年 10 月

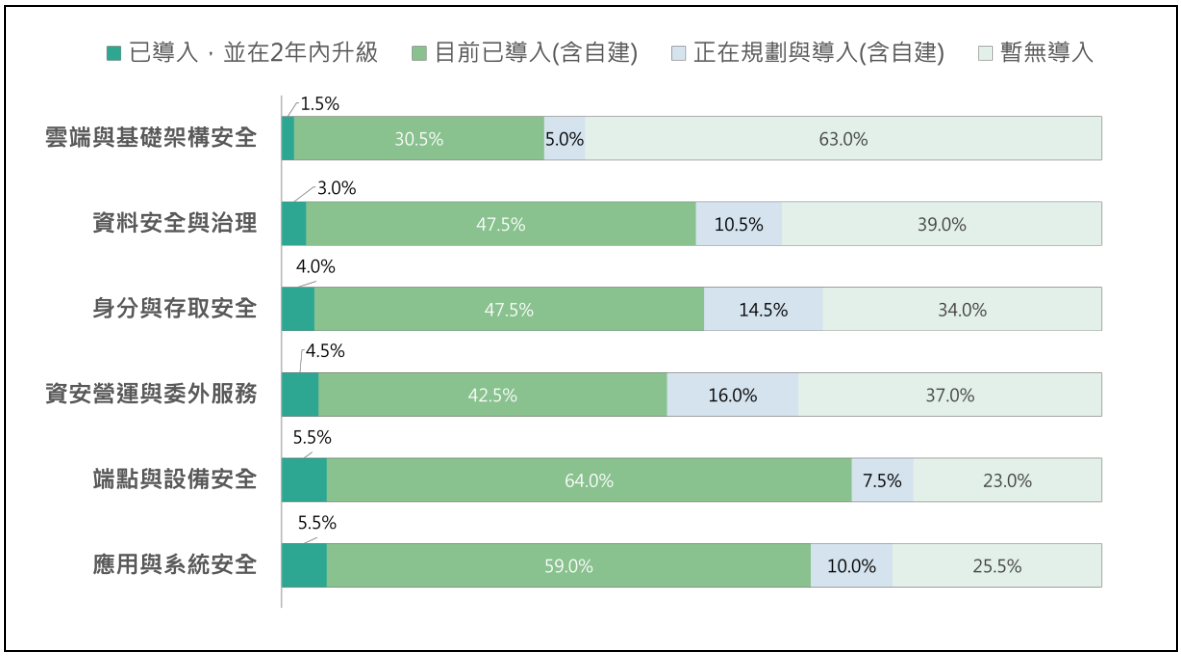
導入情形：端點與應用安全較普及，營運與存取列入規劃

以「目前已導入」及「已導入且 2 年內升級」合計來看，2026 年整體受訪業者的「端點與設備安全」導入比率為 69.5%，「應用與系統安全」為 64.5%，高於其他項目，顯示現有防護較集中於設備與應用層面。相較之下，「雲端與基礎架構安全」導入比率為 32.0%，63.0%暫無導入。惟受訪企業的部署架構與適用需求不同，尚不能僅據此判定雲端防護是否不足（參見圖十二）。

進一步觀察「正在規劃導入」的項目，「資安營運與委外服務」占 16.0%，「身分與存取安全」占 14.5%，為各項目中較高者。反映受訪製造業者的後續需求除既有防護外，也涵蓋持續監控、專業維運及存取權限管理。對地端與雲端並存的業者而言，上述措施有助於掌握跨環境的使用行為與異常，並明確銜接後續處理責任。

©2026 Market Intelligence & Consulting Institute

圖十二、2026 年台灣整體製造業各項資通安全應用與服務導入情形



註 1：整體製造業 n=200，傳統製造業 n=120，高科技製造業 n=80

註 2：各導入狀態為互斥選項；「目前已導入」不含另列的「已導入，並在 2 年內升級」者

資料來源：MIC，2026 年 10 月

採用意向：防護偵測與備援居前，治理回應選擇較少

2026 至 2027 年整體受訪製造業者預計持續使用或擴大採用的資安服務與技術，以「防護型（69.0%）」、「偵測型（58.5%）」及「備援型（49.5%）」居前，顯示阻擋攻擊、掌握異常與維持營運仍是製造業者主要需求。相較之下，「識別型」占 32.0%，「治理型」與「回應型」分別為 15.5%及 11.5%；此題最多選擇三項，結果反映相對採用意向，不等同於既有能力或實際投入程度（參見圖十三）。

「備援型」與「回應型」的選擇比重差距較大，但本調查尚未確認企業既有應變機制，或相關能力是否由委外服務提供。後續可進一步檢視備援復原與事件處置的銜接情形，並確認通報、處置及復原的權責分工，以支援營運持續。

次產業分析：傳統製造防護偵測居前，高科技識別比重較高

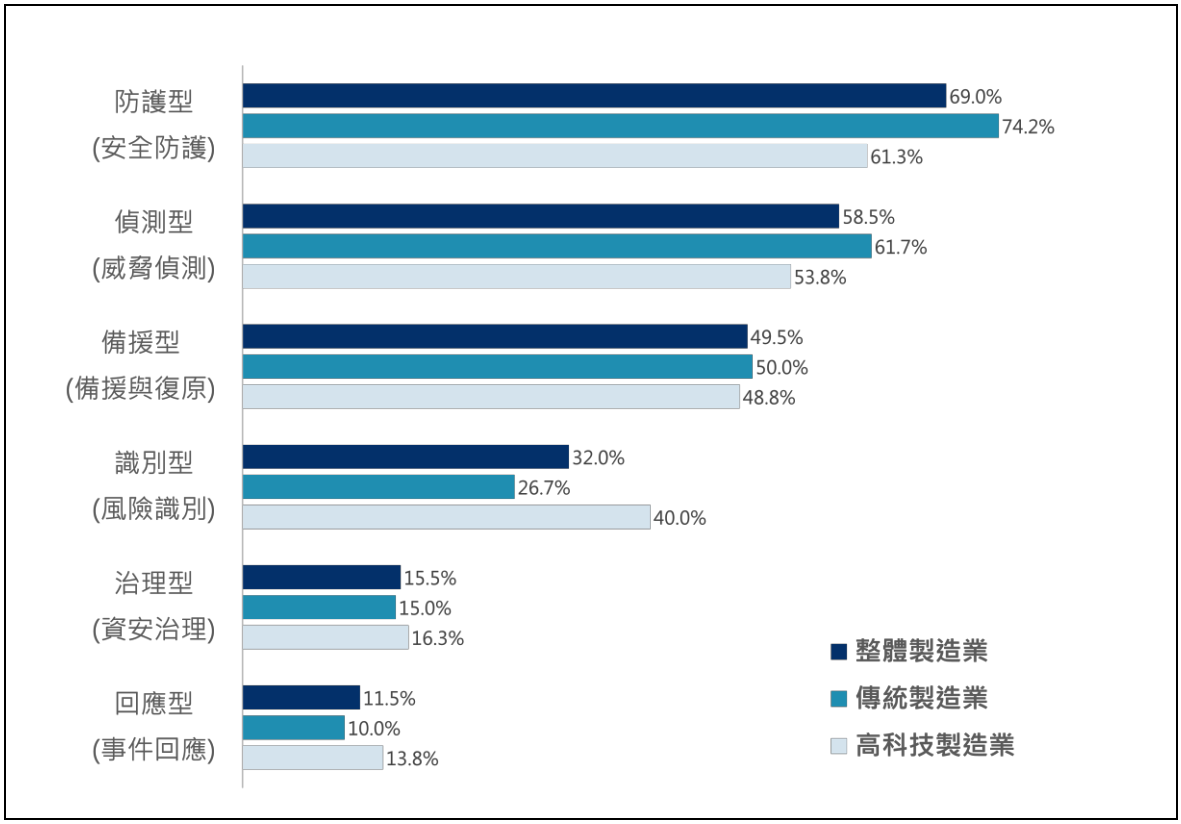
次產業方面，傳統製造業預計持續使用或擴大採用「防護型」、「偵測型」服務的比重，分別為 74.2%及 61.7%，高於高科技製造業的 61.3%及 53.8%；高科技製造業在「識別型」服務的比重則達 40.0%，高於傳統製造業的 26.7%（參見圖十三）。兩

©2026 Market Intelligence & Consulting Institute

類受訪企業的採用意向有所差異：傳統製造業選擇防護與偵測類服務的比重較高，高科技製造業則在風險識別類服務的選擇比重較高。

傳統製造、高科技製造對「備援型」服務的需求接近，皆約五成，反映復原能力是共同關注的方向。資服業者可據此調整方案重點，對傳統製造業強化防護、監控與後續處理的整合；對高科技製造業則結合風險盤點與改善追蹤，協助企業決定防護資源的配置順序。

圖十三、2026-2027 年台灣製造業預計持續使用或擴大採用的資安服務與技術



備註：整體製造業 n=200，傳統製造業 n=120，高科技製造業 n=80；此為複選題，最多 3 項

資料來源：MIC，2026 年 10 月

©2026 Market Intelligence & Consulting Institute

結論

雲端與資安支出預估增加，兩類產業增支分布有別

受訪製造業者 2027 年雲端服務與資安平均支出預估分別成長 9.3%及 7.1%。雲端平均支出的預估增幅較高，資安平均支出的預估增加金額則高於雲端服務。兩項支出皆以預估持平的企業居多，規劃增支者均未達四分之一。

其中傳統製造業支出增幅較高，但增支企業比重較低；高科技製造業則維持較大的平均投入規模，規劃增支的企業比重也較高。製造業者所提出的增支需求涵蓋應用擴充、系統升級與委外服務，授權費用及供應商調價亦影響預算安排。製造業的市場機會因此同時涉及新建置與既有服務的持續投入。資服業者可依企業的投資階段與預算用途，安排導入、升級及維運方案，使服務內容切合實際需求。

地端與雲端持續並存，服務價值延伸至AI、資料與跨環境整合

受訪企業的雲端服務支出預估增加，但資訊系統部署配置的變動相對有限，2027 年傳統地端架構的平均配置比重仍預估達 81.4%。在納入雲端服務項目分析的企業中，企業商務應用為主要選擇。兩項結果顯示，雲端服務需求與既有地端架構並存，支出增加不宜直接解讀為全面移轉上雲。

未來雲端服務增支方向涵蓋 AI 工具、資料平台及混合雲管理。傳統製造業在 AI 工具與跨環境管理的選擇比重較高，高科技製造業則在應用現代化的選擇比重較高。資服業者可依具體業務情境，確認新增應用所需的資料、既有系統介接、權限控管及維運條件，作為導入規劃與方案設計的依據。

合規與威脅帶動資安需求，治理與事件處理須銜接既有防護

法規合規與威脅事件是受訪業者調整資安預算的主要動因，服務需求因而涵蓋安全防護、查核驗證與營運保障。此外，有 55.0%的受訪業者已設置資安長或資安官，端點及應用安全也較為普及；後續重點在於將管理責任與技術措施落實為日常作業，使授權、監控及處置分工有明確依據。

受訪製造業在資安服務採用規劃上，仍以防護、偵測與備援居前，在最多選擇三項的條件下，治理及事件回應的選擇比重相對較低。隨著雲端與 AI 應用增加，資安服務可進一步串接風險盤點、監測告警、事件處理及復原作業，並建立查核證據與改善追蹤機制。建立明確的權責與一致的處理流程，有助於企業更有效運用既有防護工具，同時回應合規要求與營運持續需求。

©2026 Market Intelligence & Consulting Institute

附錄

研究方法與樣本特性

本研究針對台灣製造業之資訊長（Chief Information Officer，簡稱 CIO）或對該公司 IT 應用投資具決策權之人員進行問卷調查。調查方式以電話訪問為主，輔以傳真、Email 及郵寄等多元方式進行調查執行工作，調查執行期間為 2026 年 3 月 16 日至 2026 年 5 月 25 日止。本次調查總計完成 200 份有效樣本，有效樣本特性如下：

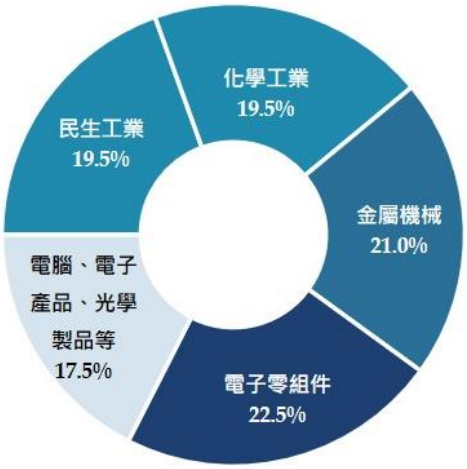
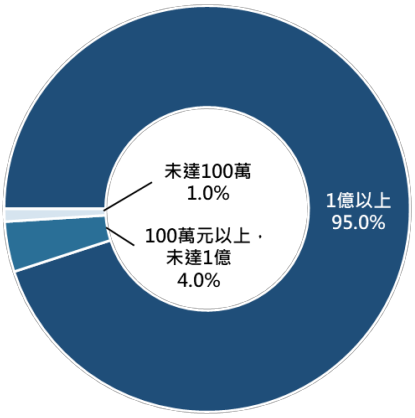
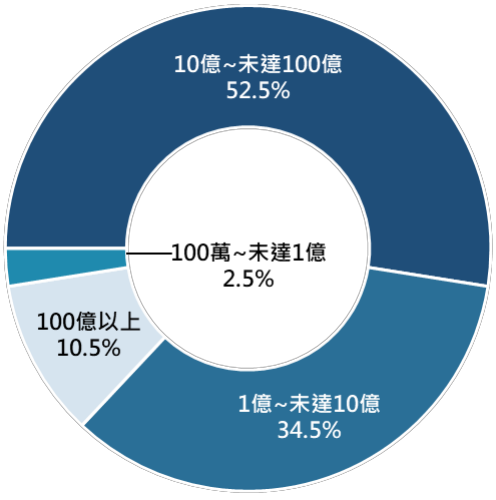
表一、整體有效樣本特性分析

項目別	說明
行業分類	傳統製造業：民生工業、化學工業、金屬機械工業 高科技製造業：電子零組件製造業、電腦 / 電子產品及光學製品製造業
產業別	傳統製造業 120 家，占 60%；高科技製造業 80 家，占 40%
2025 年 登記資本額	以 1 億元以上者占比最高(95.0%)，100 萬元以上、未達 1 億元者占 4.0%，未達 100 萬元者占 1.0%
2025 年 營業額	以 10 億元~未達 100 億元比重最高 (52.5%)，其次為 1 億元~未達 10 億元 (34.5%)，100 億元以上者占 10.5%，未達 1 億元者占 2.5%
2025 年 經常雇用員工數	以 200~499 人 (40.5%) 比重最高，其次為 100～199 人 (36.0%)，另有 23.5%業者之經常雇用員工數在 500 人以上

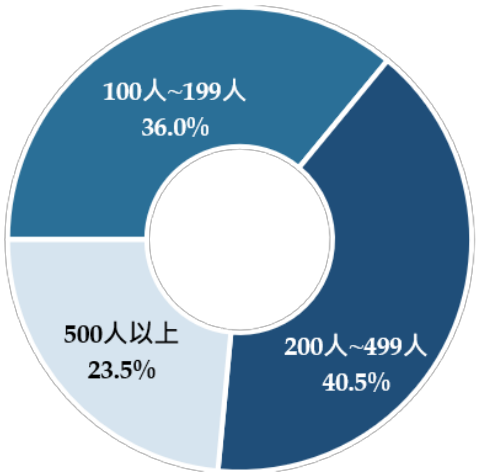
資料來源：MIC，2026 年 10 月

©2026 Market Intelligence & Consulting Institute

表二、有效樣本特性

項目別		樣本數	百分比	分布狀況（N=200）
產業別	民生工業	39	19.5%	
	化學工業	39	19.5%	
	金屬機械工業	42	21.0%	
	電子零組件製造業	45	22.5%	
	電腦、電子產品、光學製品業	35	17.5%	
2025年登記資本額	1 億元以上	190	95.0%	
	100 萬元以上、未達 1 億元	8	4.0%	
	未達 100 萬元	2	1.0%	
2025年營業額	100 萬元~未達 1 億元	5	2.5%	
	1 億元~未達 10 億元	69	34.5%	
	10 億元~未達 100 億元	105	52.5%	
	100 億元以上	21	10.5%	

©2026 Market Intelligence & Consulting Institute

項目別		樣本數	百分比	分布狀況（N=200）
2025 年經常雇用員工數	100 人~199 人	72	36.0%	
	200 人~499 人	81	40.5%	
	500 人以上	47	23.5%	

備註：依經濟部定義（109 年），經常雇用員工數係以勞動部勞工保險局受理事業最近十二個月平均月投保人數為準

資料來源：MIC，2026 年 10 月

表三、資安服務類型說明

項目別	說明
識別型	如資產盤點、攻擊面管理、安全態勢管理、持續曝險管理等
防護型	如雲端安全平台、端點 / 設備防護、網路 / 邊界防護、零信任、身分與存取管理（Identity and Access Management，簡稱 IAM）、資料防護、資料防洩漏與資料盤點等
偵測型	如端點偵測與回應(EDR)、延伸式偵測與回應(XDR)、資安營運中心(Security Operations Center，簡稱 SOC) / 日誌分析、威脅獵捕 / 紅藍隊演練、代理式 AI 防禦等
回應型	如事件應變流程(Incident Response，簡稱 IR)、電腦資安事件小組(Computer Security Incident Response Team，簡稱 CSIRT)、威脅情資整合等
備援型	如資料 / 勒索復原、備份、異地備援、業務持續計畫等

©2026 Market Intelligence & Consulting Institute

項目別	說明
治理型	如資安治理制度（ISO 27001 / 資安管理系統）、威脅建模、法規遵循（GDPR / 個資法 / 金融資安）、軟體物料清單（Software Bill of Materials，簡稱 SBOM）、第三方風險管理、AI 風險治理與控管

備註：本表補充圖十三各類服務的涵蓋範圍；分類依本調查定義，部分產品與服務可能同時涵蓋多項功能

資料來源：MIC，2026 年 10 月

©2026 Market Intelligence & Consulting Institute