發佈：2026-04-28, 週二 15:00
點擊數：57

壹、前言：國家安全層級的數位治理挑戰

在全球人工智能科技進程加速之際，新加坡與多數高度發展國家相同，正面臨數位詐騙案件急遽攀升的嚴峻挑戰。這場無聲的攻防不僅侵蝕民眾財產，更衝擊社會互信與金融體系穩定。新加坡政府已將詐騙問題提升至與反恐、反洗錢並列的國家級安全議題，展現高度危機意識與治理決心。

依新加坡官方發布之2024年統計資料，該國人口約600

萬，全年通報詐騙案件達51,501起，較前一年增加10.6%

；更令人警惕的是，年度詐騙造成之財

務總損失首度突破11億新幣（約合新台幣260億元），年增幅高達70.6%，創下新高。

面對此一趨勢，新加坡政府深刻意識到，傳統以「案發後偵查」為主的執法模式已不足以因應當前情勢。關鍵在於，2024 年高達82.4%

的案件屬於受害者在高度心理操控下的「自願轉帳」。此一現象顯示詐騙已由單純技術犯罪，演化為隱蔽性更高的社交工程與認知操控行為。

面對犯罪型態的質變，新加坡自2019

年起逐步推動結合法規調適、科技偵測與公私協力的整體戰略，試圖從源頭阻斷犯罪工具供應、在過程中即時攔截金流，並在事後強化追懲與嚇阻，建構多面向且具韌性的防詐治理體系。

本文將剖析新加坡在法制、科技與組織層面的具體作為及其成效，期為我國相關政策提供可借鏡之實務經驗。

貳、詐騙犯罪趨勢分析（2018–2024）：從量變到質變的結構性挑戰

要理解新加坡近年的政策

邏輯，必須先檢視詐騙犯罪的演化路徑。綜觀2018年至2024

年之數據，可見新加坡正面臨「損害規模極大化」、「手法心理化」與「工具虛擬化」三重結構性轉變。

發佈：2026-04-28, 週二 15:00
點擊數：57

一、案件數量與財損規模的激增

長期趨勢顯示，新加坡詐騙案件呈爆發式增長。2018年全年案件僅6,730起，至2024年已攀升至51,501起，六年間增幅高達665%，年均複合成長率約40%。此一發展反映詐騙已非偶發治安事件，而是隨數位化普及而結構性擴張的犯罪產業。

財損惡化程度更甚於案件數。2018年詐騙損失約1.51億新幣，2024年已突破11億新幣，成長逾七倍。尤其2024年呈現「量增趨緩、損失暴增」的特殊現象：案件年增率（10.6%）雖較 2020 年（64%）顯著收斂，財損金額卻暴增70.6%

1.25億新幣的驚人損失。

二、詐騙類型的分化與集中

各類詐騙在損害上呈現明顯分化，可概分為「高頻低損」與「低頻高損」兩大類：

1.高頻低損型：

以「電子商務詐騙」（如網購未到貨）為代表。2024年此類案件達11,665件，居案件數之首（占22.7%），但平均個案損失較低（約 1,508

新幣）。其主要危害在於影響面廣，長期侵蝕民眾對數位交易的信心。

2.低頻高損型：

造成國家財富大量流失者，主要為「投資詐騙」與「假冒官員詐騙」。此類案件數量未必最高，

卻因

涉及高額

資金與長時間心理

操控而成為財損主力。例如假冒官員

詐騙每案平均損失高達10

萬新幣，顯示「公權力威嚇」與「高報酬誘惑」仍是最有效的心理武器。此外，「惡意軟體詐騙

」雖案件數較少，卻因可竊取加密貨幣或銀行憑證，平均每案損失高達44萬新幣，破壞力極強。

三、心理操控與自願轉帳的常態化

過去網路犯罪多涉及駭客入侵或系統漏洞；近年趨勢則顯示攻擊目標已轉向「人性弱點」。2024

年高達 82.4%

的案件屬於受害者「自願轉帳」，意味詐騙集團透過精密的社交工程腳本（如假冒檢警、虛擬戀

人、投資導師），成功繞過傳統資安防火牆。此一「受害者高度配合」特性，使得傳統勸導或單

純雙重驗證（2FA）難以完全奏效，迫使政府必須思考更具強制性的介入工具。

四、接觸管道平台化與洗錢工具虛擬化

在接觸管道上，社群媒體與即時通訊

軟體已成為詐騙溫床。2024年資料顯示，詐騙集團高度依賴Meta旗下Facebook（占59.8%

）、WhatsApp 及 Telegram

接觸受害者。為規避追查，犯罪集團大量利用

人頭SIM卡註冊帳號，形成從接觸、誘導到洗錢的完整數位犯罪供應鏈。

在金流工具方面，加密貨幣角色日益吃重。2024

年與加密貨幣相關之詐騙損失占比攀升至24.3%

，顯示虛擬資產因匿名性與跨境轉移便利性，正快速成為詐騙與洗錢活動的核心工具，對執法機關的追查能力構成嚴峻挑戰。

圖一、新加坡詐騙犯罪趨勢分析（2018–2024）

發佈：2026-04-28, 週二 15:00
點擊數：57

參、法制架構的重塑：從被動追懲到主動介入

面對犯罪趨勢的質變，

新加坡政府認知既有法律框架存在明顯缺口，

遂於2024年至2025

年間密集修訂多項法規。其核心精神在於：賦予執法機關「提前介入」之權限，並明確化數位工具持有者與平台業者之責任。

一、源頭阻斷：斬斷數位身分與通訊工具的黑市供應

發佈：2026-04-28, 週二 15:00
點擊數：57

針對詐騙集團高度依賴的人頭帳戶與通訊工具，新加坡採取「源頭阻斷」的立法策略。過去檢方往往難以證明提供帳戶或SIM卡者「明知」其用於犯罪，致使人頭戶長期遊走法律邊緣。

修訂後之《電腦濫用法》與《雜項犯罪法》扭轉此一困境：新法將提供或濫用數位身分（如Singpass）、SIM
卡代辦、人頭註冊等行為明確入罪；且不再以「明知」為必要要件，只要構成「魯莽」或「過失」——例如為微薄報酬交出帳密，或電信員工濫用客戶資料——即可能成立犯罪。

此一設計顯著降低
主觀構成要件之舉證門檻，並迅速反
映於執法成果：警方於2025年3
月依新修訂《雜項犯罪法》
查獲電信門市員工盜用客戶資料註冊人頭SIM卡案，同年7月更逮捕44
名涉嫌偽冒註冊SIM卡者，凸顯新法之即時嚇阻效果。

二、平台治理：賦予政府對科技巨頭的指令權

在平台治理方面，跨境數位平台過往對詐騙內容處置往往消極且滯後。新制定之《網路犯罪危害法》（OCHA
）賦予政府對大型網路平台發布具法律效力之「指令」權限，得採取「帳戶限制」、「內容封鎖」，甚至「應用程式下架」等措施。

發佈：2026-04-28, 週二 15:00
點擊數：57

內政部於 2025 年 9 月與 11 月分別對 Meta、Apple 及 Google

發出實施指令，要求即時移除詐騙帳號、封鎖內容或攔截冒充政府之簡訊；平台若不配合，將面臨高額罰款。此一制度意味平台業者不再能以「技術中立」作為卸責理由，而須承擔數位守門人之治理責任。

在此機制帶動下，2024

年新加坡警方與平台合作，成功阻斷逾17

萬組詐騙相關電話線路、網站與社

媒帳號，較前一年大幅增加719%，展現強化主動防禦的政策取向。

三、強制介入：突破心理操控的「限制令」

針對逾八成案件屬「自願轉帳」之現實，傳統勸導往往力有未逮。新制定的《防詐騙保障法》因而賦予警方關鍵工具——「限制令」。

當警方認定民眾處於高度受操控風險情境下，即便其仍堅持匯款，執法機關亦可強制通知銀行暫停帳戶轉帳、ATM 提款與信貸等功能，凍結期限最長可達 180

天（含延展）。截至2025年8月，警方已實際發出限制令以凍結潛在受害者帳戶。

此一措施確實介入個人財產處分自由，但也反映新加坡在法益衡量上，將「防詐保全」置於更高順位，以突破「只能勸、不能擋」的執

法困境。數據顯示2025

年上半年受害者自願轉帳比率已由前一年86.1%降至78.8%，顯示強制介入措施已初見成效。

四、金流監管與嚴刑峻罰

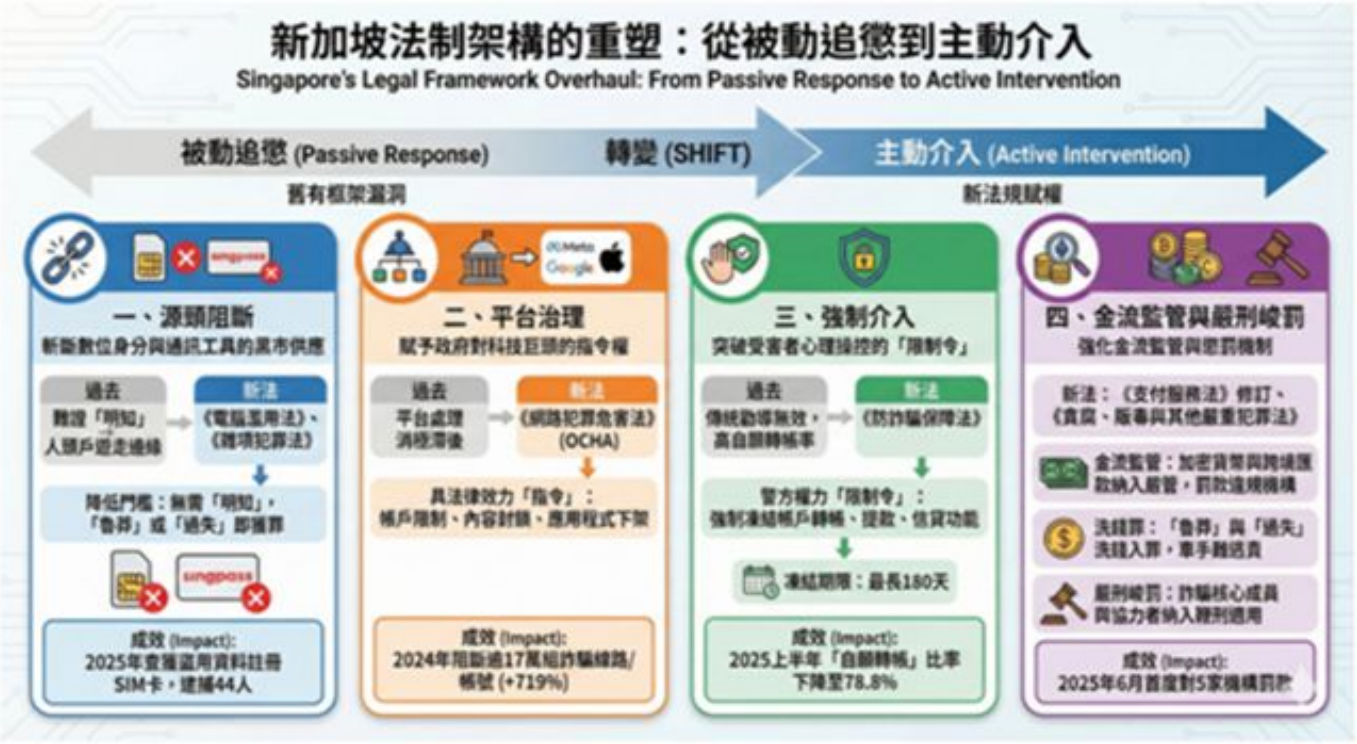
在金流監管與懲罰面，新加坡透過修訂《支付服務法》，將加密貨幣與跨境匯款納入更嚴格之監理範圍。金管局於2025年6月首度依該法對 5
家未盡合規查核義務之支付機構處以罰款，展現監理決心。

同時，《貪腐、販毒與其他嚴重犯罪（沒收利益）法》增設「魯莽」與「過失」洗錢罪，即使車手主張不知情，只要未盡合理查證義務，仍可能構成犯罪。

刑罰方面，新加坡亦透過《刑事法（雜項修正）法案》，將詐騙主謀、核心成員與協力者納入鞭刑適用範圍，以具高度象徵性的嚴刑峻罰，強化對犯罪集團的威嚇效果。

圖2、新加坡法制架構的重塑

發佈：2026-04-28, 週二 15:00
點擊數：57



肆、科技應用的轉型：從被動查詢到 AI 主動獵殺

在法制賦權基礎上，新

加坡科技防詐策略已由早期的被動宣導，轉型

為以AI為核心的主動偵測與即時阻斷，力求在詐騙訊息接觸民眾之前即予攔截。

一、全民數位防線：ScamShield 套裝的演進

最具代表性的成果之一，是全民防詐工具ScamShield的升級與普及。ScamShield由原本單一手機

App

，擴充為整合熱線、網站與通訊平台

的完整防詐套裝，並以AI自動過濾詐騙簡訊與來電，支援一鍵通報。截至 2025

年，下載量已突破 135 萬次，成為全民防詐第一道數位防線。

為對抗假冒政府之釣魚簡訊，新加坡政府全

面導入「gov.sg

」單一簡訊識別碼，要求電信商強制攔截所有未授權發送者，確保政府簡訊來源唯一。依統計，

截至2025年6月，透過該機制發送逾1.8

億則簡訊，未發生任何遭偽冒案例，顯著重建民眾對官方訊息之信任。

二、網域獵殺系統：SATIS 的主動防禦

面對釣魚網站層出不窮，

新加坡開發「詐騙分析及戰術性介入系統」（SATIS），每日自動掃描逾十萬個網站，並以 AI

分析網頁結構與內容，以辨識釣魚連結與假冒平台。一旦判定風險，系統即與搜尋引擎（如

Google）及社群業者合作，即時封鎖，避免詐騙內容在大規模擴散後才被動處理。

僅 2024 年，SATIS 即成功下架近 4.5 萬個詐騙網站與 4 萬多個 WhatsApp

帳號；攔阻效率較前一年分別成長 79% 與

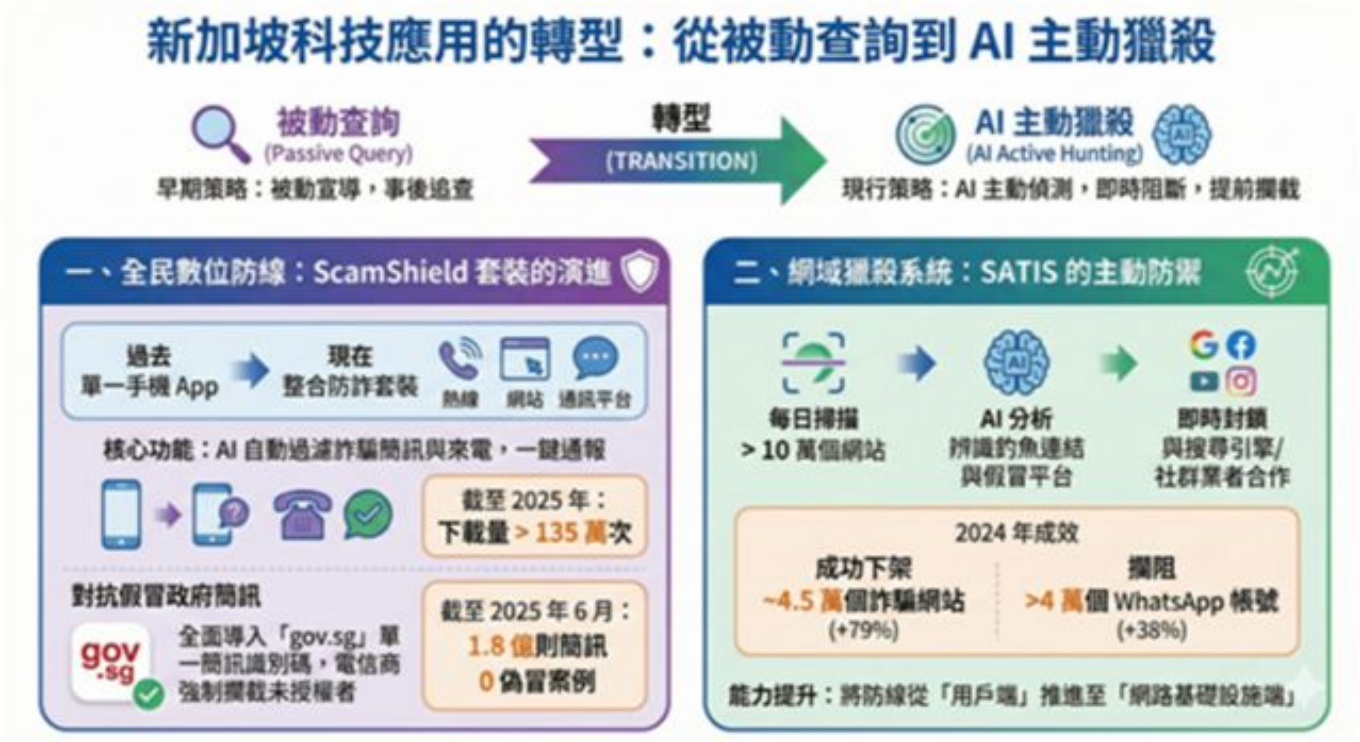
38%

。此一成果反映新加坡已能將技術偵測快速轉化為具體治理行動，將防線由「用戶端」前推至「

網路基礎設施端」。

發佈：2026-04-28, 週二 15:00
點擊數：57

圖3、新加坡科技應用的轉型



伍、公私協力的實踐：跨域聯防與責任分擔

新加坡防詐體系能有效運作，其關鍵在於高度制度化的公私協力機制。此一協力不僅止於倡議口號，而是落實為合署辦公、資訊共享與責任分擔的具體制度設計。

一、實體合署辦公：反詐騙指揮處的高效運作

在組織層面，反詐騙指揮處（ASCom

）整合警方、七大系統性銀行（如星展、大華、華僑）與大型電商平台（如

Carousell、Shopee

）代表合署辦公。此一「實體進駐」模式打破跨機構溝通壁壘，使銀行人員可即時配合執法需求

。過往需數日公文往返方能凍結之資金，得以壓縮至近乎即時處理。

2024 年 ASCom 因此成功追回逾1.82

億新幣受害款項，並額外攔阻約4.83億新幣的潛在損失，顯示合署辦公對降低財損具直接效益。

二、金融責任架構：迫使銀行主動防禦

制度層面上，2024

年底新加坡實施「共同責任架構」，堪稱全球金融監理的重要創新。該架構要求金融與電信業者分擔釣魚詐騙的賠償責任，並以「瀑布式」究責機制明確界定責任歸屬，迫使銀行與電信業者主動升級防護措施。

在此壓力下，銀行導入「資金鎖定」（Money

Lock

）功能，允許用戶將存款「上

鎖」，使其無法透過網銀轉帳。截至2025年6月，已有逾37

萬名客戶啟用，鎖定逾300

億新幣資產。此外，銀行亦全面取消易遭攔

截之簡訊OTP

，改採數位憑證驗證，並對高風險轉帳設置冷卻期，以降低被操控下的即時匯款風險。

三、自動化預警與社區聯防

警方與銀行合作推動「星空智速反詐」（Project

A.S.T.R.O.

）計畫，透過自動化技術分析潛在

受害特徵並發送簡訊預警。2024年該系統發送逾7.7萬則簡訊，成功預警5.5

萬名潛在受害者，攔阻約4.2

億新幣的潛在損失，顯示科技可有效補足人力宣導的覆蓋與即時性不足。

在社區層面，政府亦透過樂齡防詐志工與自動化預警，將防詐觸角延伸至鄰里與日常生活場域，形成線上線下交織的防護網。例如「樂齡防詐計畫」以同儕志工深入社區，已在第一線成功勸阻多起長者遭操控匯款案件，反映社會動員仍是面對心理操控型詐騙的重要支柱。

圖4、新加坡公私協力的實踐

發佈：2026-04-28, 週二 15:00
點擊數：57

陸、打詐政策成效評估與結語

總結新加坡近年的防詐經驗，雖2024

年詐騙案件總數仍創新高，但若進一步檢視各項指標，其綜合治理模式已產生實質抑制效果。

首先，案件增長勢頭已明顯趨緩。年增率由過去倍數或高雙位數增長，收斂至

2024年的10.6%

。在詐騙手法持續翻新的背景下，此一收斂趨勢意味防護體系已具一定緩衝與吸收衝擊的能力。

其次，強制介入措施開始展現政策效果。隨《防詐騙保障法》及限制令制度上路，受害者「自願

轉帳」比率已由前一年86.1%降至2025年上半年之78.8%

。此一變化顯示，對深陷心理操控之受害者，公權力的適時介入確能有效阻斷資金外流。

再者，資金攔阻與追回成果屢創新高。2024

年警方與銀行合作攔阻及追回款項合計逾6.65

億新幣，顯示公私協力機制在降低實際財損上扮演關鍵角色，也凸顯合署辦公與資訊共享對治理效能的加乘效果。

然而，挑戰依然存在。財損集中化現象顯示，針對高資產族群的精準詐騙（如惡意軟體、假冒官員）仍具高度破壞力；加密貨幣詐騙占比快速攀升（達

24.3%

Telegram等加密通訊軟體，亦對平台監理與內容治理提出新的技術與法制難題。

新加坡經驗的核心價值，在於其跨部門快速整合能力與務實、彈性的法規調適策略。面對詐騙集團

不斷

演化，新

加坡不倚賴單一手

段，而是透過法規賦權（限制令、平

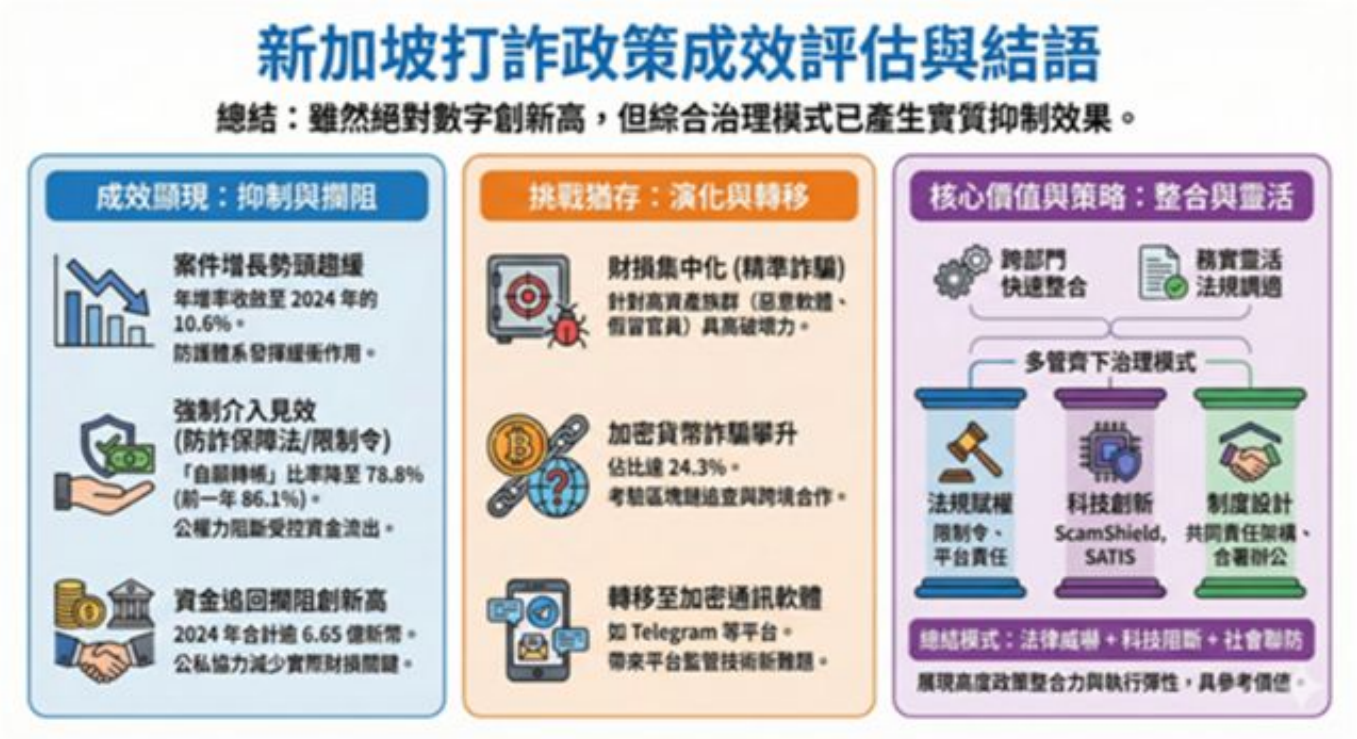
台責任）、科技創新（ScamShield、SATIS

發佈：2026-04-28, 週二 15:00
點擊數：57

）與制度設計（共同責任架構、合署辦公）多管齊下，形成「法律威嚇—科技阻斷—社會聯防」的整合治理模式。

對同樣面臨高科技詐騙威脅的台灣而言，新加坡的作法提供了可具體對照與借鏡的政策參考：在保障個人權益與降低社會財損之間，如何以制度化工具提升即時攔阻能力，並透過責任分擔機制促使公私部門共同承擔治理義務，將是未來防詐政策設計的關鍵課題。

圖5、新加坡打詐政策成效評估與結語



發佈：2026-04-28, 週二 15:00
點擊數：57

作者 童振源 博士 為 駐新加坡代表