新加坡防制詐騙的整合治理模式對台灣的政策啟示

蔡錕銘*

摘　要

本文以新加坡為案例，探討其面對數位詐騙威脅時，如何透過整合治理模式有效回應挑戰，並試圖分析其制度設計、科技應用與國際協力對防詐成果之貢獻，進一步思考此經驗對台灣的政策啟示。根據《Annual Scams and Cybercrime Brief 2023》資料，新加坡 2023 年詐騙與網路犯罪案件總數超過五萬件，雖案件數激增，總損失金額卻較前一年下降 1.3%，反映出其政策成效。新加坡透過設立「反詐指揮部」（ASCom），結合警政、通訊、科技與金融機構，實施如即時凍結帳戶、封鎖詐騙網站與發送預警簡訊等措施，有效減少潛在損失。此外，政府重視公民教育，推行「我能ACT」宣導計畫，並發展ScamShield等數位工具，提升全民數位素養。法律面亦透過《線上犯罪危害法》等修法強化對平台與犯罪行為的規範，並推動與國際刑警組織等跨國合作，成功摧毀 19 個境外詐騙集團。本文最後對比台灣現況，指出台灣雖已組建「打詐國家隊」，但仍在跨部門整合、科技應用與社群平台監理等層面存在不足。新加坡經驗顯示，防詐成敗取決於是否能將治理視為一場長期數位戰役，並在法規、制度、文化與技術上全面備戰。唯有如此，台灣才能真正從防守轉為主動，保護人民財產與信任。

關鍵字：新加坡、詐騙防制、數位治理、跨部門協作、網路犯罪、台灣政策借鏡
JEL **分類代號：**K42, H83, O38, L86

* 淡江大學財務金融學系兼任教授，台北張老師基金會副主任委員

壹、導論

近年來，台灣社會飽受詐騙所苦。從假投資、電商詐騙，到冒充親友的即時通訊騙局，層出不窮的手法讓民眾防不勝防。根據《165 打詐儀錶板網站》2024 年全台詐騙財損金額，光是 165 打詐儀錶板上路後的 8 到 12 月，受理件數達 93,379 件，財損金額高達 629 億元，推算全台整年詐騙金額至少破千億元。其中以假投資真詐騙為最常見手法，2025 年 1 到 4 月累計受理件數即高達 56,497 件，累計財損 303.7 億元。即便政府近年已啟動「打詐國家隊」，並推出 165 反詐騙諮詢專線與各類通報管道，但詐騙案件數與手法仍不斷翻新，顯示目前防詐策略在制度整合與科技應用上仍存諸多挑戰。

與此同時，新加坡亦面臨高度數位化下的詐騙風險，惟其政府透過制度化、整合化與科技化的治理模式，實現了在詐騙案件大幅增加的同時，損失金額首度下降的成果。本文將以新加坡防制詐騙的整合治理模式為分析核心，探討其制度設計、科技應用與法治策略如何形成完整的應對體系，並進一步思考其經驗對台灣當前防詐政策之借鏡與啟示。

貳、新加坡的詐騙樣態與風險輪廓

新加坡的網路詐騙與相關犯罪近年快速攀升：根據官方統計，2019 年整體網路犯罪案件僅 11,135 件，到 2023 年已增至 50,376 件，五年間成長超過 352%。其中，單是詐騙案件就達 46,563 件，占整體網路犯罪的 92.4%，凸顯詐騙問題已成主要威脅。不過，雖然詐騙案件數攀升，但整體損失金額卻呈現微幅下降，反映出其政府在防詐作為上展現初步成效。

觀察詐騙類型，2023 年五大詐騙手法分別為：

一、求職詐騙（Job Scam）

案件數高達 9,914 件，為各類型之冠。詐騙手法包括假冒人力資源公司招攬在家打工機會，要求先行付款以「購買任務」，再以虛假獲利吸引受害者投入更多資金。總損失金額高達 1.36 億新幣，平均每案損失約 13,692 新幣。

二、電商詐騙（E-commerce Scam）

案件數為 9,783 件，受害者多透過Facebook、Carousell與Telegram購物，遭遇假賣家收錢不出貨，總損失約 1,390 萬新幣。

三、假冒朋友來電詐騙（Fake Friend Call Scam）

此類案件暴增 225.7%，達 6,859 件。騙徒冒用熟人身份來電，誘騙受害者匯款，平均損失為 3,373 新幣。

四、釣魚詐騙（Phishing Scam）

案件數為 5,938 件，透過假冒政府機關或銀行網站、簡訊連結誘導輸入個資，造成財務損失達 1,420 萬新幣。

五、投資詐騙（Investment Scam）

雖案件數相對較少，僅 4,030 件，但平均每案損失達 50,754 新幣，總損失金額突破 2 億新幣，為金額損失最重之類型。

這些詐騙手法多數利用社交平台與即時通訊軟體接觸受害者。新加坡警察部表示，2023 年透過社交媒體聯絡受害者的案件達 13,725 件，較 2022 年大增 82%。其中 71.7%透過Facebook、18.5%來自Instagram，顯示社群平台已成詐騙熱區。

此外，詐騙受害者年齡層集中於 30 至 49 歲，占整體 43.1%。這群人因生活忙碌、線上交易頻繁，反而成為高風險族群。尤其「以利誘為主」的詐騙話術，如高薪兼差、快速獲利、限時優惠等，在這一族群中最具吸引力。

本章節資料與數據來源為 2024 年 2 月新加坡警察部發布的《Annual Scams and Cybercrime Brief 2023》，屬官方統計，具高度參考價值。綜觀新加坡詐騙現況，可發現其挑戰與台灣類似，但其防範之道卻頗具制度與創新特質，以下章節概述之。

參、整合全政府資源：新加坡打詐的跨部門策略

新加坡對詐騙的因應，並非零星措施或個別單位行動，而是採取「全政府、跨部門、聯合民間」的整合策略。這種打詐架構不僅提升應變效率，也成為其減緩詐騙損失的關鍵。

一、成立「反詐指揮部」與跨機構合作機制

新加坡於 2022 年成立「反詐指揮部」（Anti-Scam Command, ASCom），其功能相當於打詐總部，隸屬新加坡警察部商業事務局。該機構不僅整合警力，更與新加坡資訊通訊媒體發展局（IMDA）、新加坡網路安全局（CSA）、金管局（MAS）、Smart Nation Group 及多家金融機構、科技公司建立即時合作通道。

截至 2023 年，反詐指揮部已與超過 100 家本地與國際機構合作，包含銀行、加密貨幣交易平台、電信商與電商平台，共同建立「即時凍結帳戶與追回資金」機制。根據《Annual Scams and Cybercrime Brief 2023》指出，該指揮部一年內成功凍結超過 19,600 個銀行帳戶，追回金額超過 1 億新幣。

二、強化數據共享與即時監控系統

新加坡反詐作為的一大特色在於高度的數據整合能力。例如，ASCom與政府科技局（GovTech）共同建置系統以即時偵測Singpass（新加坡的國民數位身份系統）異常活動。政府並允許多家銀行派員常駐指揮部，實現從通報、比對到資金凍結的「一站式處理」。

此外，2023 年新加坡推出自動化打擊詐騙戰術與警示計畫「Project A.S.T.R.O.」（Automation of Scam-fighting Tactics & Reaching Out），透過自動化方式與各大銀行共享可疑交易名單，再以簡訊方式主動提醒潛在受害者。在六次行動中共發出逾 6.8 萬則警告簡訊，成功避免 2.85 萬人受騙，潛在挽回損失達 1.48 億新幣。

三、整治通訊管道與數位廣告

為遏止詐騙的傳播途徑，新加坡政府會同IMDA與本地電信業者，在 2023 年關閉超過 9,200 支手機門號與 29,200 個WhatsApp帳號，並要求所有未登記的簡訊發送帳號標註為「Likely-SCAM」。同時，針對詐騙網站，新加坡警方與網際網路服務提供商（Internet Service Provider, ISP）合作，一年內封鎖超過 25,000 個詐騙網址。

這些政策展現出新加坡政府在數位治理上的高效能，並證明當局不是被動封鎖，而是主動追蹤、精準打擊、結合科技，進行「預防式治理」的實踐。

肆、全民教育與科技應用：由下而上的反詐文化建構

除制度與科技之外，新加坡政府亦投注相當多資源於民眾教育與數位素養培育，建立「全民反詐文化」，讓每個人都成為第一道防線。

一、「我能ACT」宣導與多語言接觸策略

為讓民眾能辨識詐騙，新加坡國家犯罪預防理事會（NCPC）與警察部合力推動「我能ACT對抗詐騙」（ACT = Add, Check, Tell）行動計畫。該計畫內容簡明扼要，主張：

(一) Add：新增官方通訊管道與反詐工具，如 ScamShield。

(二) Check：多方查證來源真實性。

(三) Tell：向警方通報可疑訊息或協助親友。

「我能ACT」影片與歌曲已在社群平台累計逾百萬次瀏覽，並廣泛應用於校園課程與長者活動中。政府透過多語言推廣，確保英語、華語、馬來語、泰米爾語等社群皆能接收到訊息，展現新加坡語言政策優勢。

二、ScamShield 與數位工具應用

在工具層面，政府推出ScamShield應用程式，自推出至今已超過 85 萬次下載，使用者舉報的可疑簡訊超過 790 萬則。透過AI演算法與群眾回報數據，ScamShield能自動過濾與封鎖潛在詐騙簡訊與來電，顯示出「集體資料」在防詐策略中的實用價值。

此外，ScamAlert網站、WhatsApp與Telegram頻道定期更新最新詐騙案例與手法，使民眾能與詐騙技術進展「同步對抗」。

三、精準教育與社群參與

新加坡亦強化對不同年齡與族群的專屬教育，例如：

(一) 對 50 歲以上長者，與各社區組織合辦「歌台＋反詐宣導」活動；

(二) 對移工群體推出「家庭守護者計畫」，培訓其反詐意識；

(三) 校園定期辦理「Be Cyber Safe」劇場與互動展覽，提高學生網路安全意識；

(四) 成立「E-Shoppers on Watch」興趣小組，邀請網購族協助警方蒐報線索。至 2023 年底，該小組已有 7,700 名會員，年增幅高達 79.1%，展現出群體參與的潛力。

全民教育與技術應用不僅是輔助手段，而是新加坡反詐策略的根本基礎之一。它不只是「防守」，更是透過持續學習與社會參與，逐步構築出能與詐騙對抗的數位公民社會。

伍、法律制度與國際合作：打詐的制度支撐與跨境協力

在數位詐騙迅速跨越國界的當下，單靠國內措施難以全面防堵。新加坡正視這一現實，逐步強化法律工具與國際執法合作，為打詐行動提供制度支撐與跨境打擊力道。

一、修法與法源完備

2023 年，新加坡國會修訂多項重要法案，包括：

(一) 《線上犯罪危害法》（Online Criminal Harms Act）：2024 年 2 月起實施，授權警方對平台提出指令，要求其禁止詐騙帳戶與內容觸及新加坡用戶；也可要求平台進行實名驗證等安全措施。

(二) 《電腦濫用法》（Computer Misuse Act）與《貪污、毒品與嚴重犯罪沒收利益法》（Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act, CDSA）亦於 2023 年 5 月完成修訂，強化對濫用Singpass帳號與洗錢「人頭帳戶」的刑責。

同時，政府計畫推出「濫用SIM卡罪」條文，打擊協助詐騙集團透過預付門號隱匿身份的中介行為。這些修法展現新加坡對新型詐騙手法與科技濫用的高度警覺。

二、國際合作與跨境行動

新加坡反詐也強化與國際執法單位的合作。2023 年，新加坡警方參與兩項由國際刑警（INTERPOL）主導的跨國行動：

(一) 「晨光行動」(Operation First Light)：涵蓋 76 個國家，新加坡共凍結 5,300 個帳戶，追回超過 1,150 萬新幣資金。

(二) 「海氣行動」(Operation HAECHI)：涵蓋 32 國，新加坡查處逾 800 名涉案嫌疑人，凍結 4,900 個帳戶，查扣虛擬資產逾 50 萬新幣。

另根據 2023 年統計，新加坡警方與海外執法機關合作，成功摧毀 19 個境外詐騙集團，涉及超過 730 件案件，逮捕超過 110 人。這些成果凸顯一國打詐成效，往往取決於跨國司法協助與資訊共享能力。

三、公私合作、責任共擔

新加坡政府也將反詐責任擴及民間平台與企業，舉例而言：

(一) Facebook Marketplace因未落實用戶驗證制度，被評為最差的「一勾」(一星)等級；

(二) 反觀Amazon、Lazada與Qoo10 因導入政府建議的驗證與交易保障機制，則獲得「四勾」(四星)評級；

(三) 金融機構則推出「Money Lock」功能，允許用戶將資金鎖定，避免被詐團盜轉。截至 2024 年 1 月，已有逾 4.9 萬個Money Lock帳戶成立，保護資金總額逾 42 億新幣。

這些制度設計與機制實踐，顯示政府透過政策工具促使平台主動管理風險，真正實現「打詐不是警察的事，而是全民與平台的責任」。

陸、結語

綜觀新加坡的防詐經驗，我們可清楚看見一個整合治理模式的成功實踐樣貌。其關鍵不僅在於技術與法規，更在於整體制度設計的前瞻性與執行力。從ASCom的跨機構協調到ScamShield的科技部署，從ACT公民教育到《線上犯罪危害法》的法治基礎，新加坡建立了一套具有預警、防堵與應變功能的整合體系。

對台灣而言，當前防詐策略已具雛形，但在制度整合與資源配置上仍有落差。本文建議，台灣可從以下四個方向，借鏡新加坡經驗進行政策強化：

一、設立常設性跨部門反詐平台：如同新加坡 ASCom，台灣可整合內政部、數發部、金管會與NCC等機關，設立具法定地位的「國家反詐治理中心」，提升指揮與應變效能。

二、發展預警性科技工具與即時資料共享機制：建置類似ScamShield、Project A.S.T.R.O.的台灣版本，並促成警方與金融機構、通訊業者之間的即時異常交易通報與攔阻機制。

三、強化平台治理責任與透明度：參照新加坡的「交易安全評比」（TSR）制度，要求Facebook、LINE、Shopee等高風險平台公開其防詐作為，並接受第三方監督。

四、制度化全民教育機制：除推動校園教育與長者宣導外，可仿效E-Shoppers on Watch模式，發展在地化社群志工體系，讓防詐知識透過社群網絡擴散。

新加坡的整合治理模式顯示，防詐已非單一警政問題，而是關乎數位社會安全、信任機制與治理能力的國家議題。唯有將防詐納入國家治理結構，並落實於制度、科技與文化層面，才能真正從防守轉向主動，讓全民信任與財產安全不再淪為詐騙集團的獵物。

參考文獻

165 打詐儀錶板網站, https://165dashboard.tw/

Smart Nation Singapore, 「Smart Nation 2.0」,https://a16.hm-f.jp/cc.php?t=M744442&c=52219&d=a05a

SINGAPORE POLICE FORCE, 「Annual Scams and Cybercrime Brief 2023」, https://a16.hm-f.jp/cc.php?t=M744443&c=52219&d=a05a

JETRO《商務簡報》（2024 年 10 月 7 日發行）, 「智慧國家計畫啟動十年，目前已進入第二階段」, https://a16.hm-f.jp/cc.php?t=M744444&c=52219&d=a05a

知新聞，「2024 遭詐破千億！假投資最惡奪 4 命　這縣市人均被騙最多錢」，2025.01.11. https://www.knews.com.tw/news/E15B6460FB66AF5ECC707AB035B05C8B

補佐坂本 「シンガポールの詐欺被害防止への取り組み」，2025.02.21. https://www.clair.org.sg/j/mail-magazine/%e3%80%90%e3%82%b7%e3%83%b3%e3%82%ac%e3%83%9d%e3%83%bc%e3%83%ab%e4%ba%8b%e5%8b%99%e6%89%80%e3%80%91%e3%82%b7%e3%83%b3%e3%82%ac%e3%83%9d%e3%83%bc%e3%83%ab%e3%81%ae%e8%a9%90%e6%ac%ba%e8%a2%ab%e5%ae%b3/

著作財產權同意書

本同意書人（即著作人）所作刊載於「臺灣銀行季刊」（第　卷第　期）中之＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿一文，著作人享有著作財產權，同意於該文著作財產權存續期間，授與臺灣銀行重製權、散布權及公開傳輸權，享有在任何地點、任何時間以任何方式利用（包括但不限於數位方式出版、登載於臺灣銀行全球資訊網供外界參閱）或再授權他人利用該著作之權利，且臺灣銀行不需因此支付任何費用。

著作人擔保本著作係著作人之原創性著作，僅投稿「臺灣銀行季刊」，且從未出版過。若本著作之內容有使用他人受著作權保護之資料，皆已獲得著作權人（書面）同意，或符合合理使用規定於本著作中註明其來源出處。著作人並擔保本著作未含有誹謗或不法之內容，且未侵害他人之權利。

若本著作為二人以上之共同著作，下列簽署之著作人亦已通知其他共同著作人，本同意書之條款，並經各共同著作人全體同意，且獲得授權代為簽署本同意書。

立同意書人（即著作權人之姓名）：　　（簽章）

身分證統一編號：

戶籍地址：

聯絡電話：

電子郵件信箱：

中華民國　　年　　月　　日