公務出國或赴大陸地區報告（出國類別：考察）

新加坡 AI 與資安治理考察報告

服務機關：臺中市政府數位發展局

姓名職稱：林谷隆局長等 3 人

派赴國家：新加坡

出國期間：114 年 12 月 16 日 至 114 年 12 月 19 日

報告日期：115 年 2 月 6 日

目錄

壹、 摘要 1

貳、 出國人員名單 2

參、 目的 3

肆、 過程 5

一、 參訪行程表 5

二、 新加坡國立大學計算機學院 6

三、 亞洲台灣商會聯合總會青商會 9

四、 Amazon Web Services（AWS）亞太總部 11

五、 拜訪駐新加坡代表 16

六、 CISCO 亞太總部 19

七、 新加坡個人資料保護委員會 23

伍、 心得 27

陸、 建議 31

壹、摘要

為強化智慧城市發展與資通安全治理，臺中市政府數位發展局再度參訪新加坡，取經新加坡推動「智慧國（Smart Nation）」政策下，在資安防護、個資保護及生成式 AI 風險管理的最新實務。學習新加坡在資通安全、個人資料保護法制及生成式 AI 風險管理方面的領先經驗。

參訪首站拜會新加坡國立大學計算機學院，就學術觀點進行討論。在產業實務方面，考察團走訪亞馬遜雲端運算服務 AWS 亞太總部，研析其 Nitro 系統的物理隔離安全技術、零信任架構及協助新加坡政府推動「Singpass」數位身分認證的實務路徑。隨後於 Cisco 亞太總部觀摩分散式 AI 資料中心藍圖、AI 原生安全防禦技術及深偽偵測機制，藉此強化臺中市數位服務的防詐能力與數位韌性。

在法制治理層面，團隊拜會新加坡個人資料保護委員會，瞭解其《個資法》之執行、企業資料保護官制度以及兼顧創新與合規的平衡機制。此外，透過與駐新加坡代表處童振源大使及亞洲台商總會青商會的交流，開拓臺中市數位人才與國際大廠接軌的合作管道。此次考察成果將作為本市數據治理政策的重要參考，致力打造更安全、便捷的智慧台中。

貳、出國人員名單

序號	機關單位	職稱	姓名
1	臺中市政府數位發展局	局長	林谷隆
2	臺中市政府數位發展局 網路資安科	分析師	陳榮州
3	臺中市政府數位發展局 整合應用科	分析師	黃兆農

參、目的

隨著人工智慧（AI）技術的指數級成長與生成式 AI 的廣泛應用，全球智慧城市的治理模式正面臨前所未有的轉型壓力與資安挑戰。臺中市政府積極推動數位轉型，致力於將臺中打造為安全、便捷且具備數位韌性的智慧城市。新加坡作為全球公認的「智慧國（Smart Nation）」典範，其在數位政府、資通安全、個人資料保護及 AI 風險管理上的實務經驗，極具參考價值。

本次考察之主要目的，在於深入了解新加坡如何透過「產、官、學」三方協作，構建具備高度韌性的國家級數位基盤，並具體聚焦於以下三大核心面向：

一、 掌握前瞻 AI 與資安技術趨勢，強化數位防禦

本次考察旨在向新加坡國立大學及國際科技大廠取經，了解「零信任架構」、「機密運算」及「AI 原生資安」等前瞻技術。透過了解 AWS 的 Nitro 物理隔離技術與 Cisco 的 Hypershield 防禦機制，以提升對抗深偽詐騙及新型態網路攻擊的防禦能力。

二、 精進資料治理與個資保護機制

數據是發展 AI 的核心燃料，如何在創新應用與隱私保護間取

得平衡，是政府治理的關鍵課題。本次參訪新加坡個人資料保護委員會（PDPC）及 NUS 計算機學院，目的在於學習新加坡《個人資料保護法》（PDPA）的執行實務、企業資料保護官（DPO）制度，以及學術界在「差分隱私」上的最新研究。這些經驗將作為本府精進數據治理政策，以及未來修訂相關管理規範的重要參據。

三、 拓展國際數位合作網絡，深化人才培育

除技術層面外，本次亦透過拜會駐新加坡代表處及亞洲台灣商會聯合總會青商會。透過了解新加坡政府的人才培訓模式及各國際大廠的教育訓練資源，尋求建立長期的數位人才培育機制。

肆、過程

一、參訪行程表

日　　期	行　　程
12 月 16 日 （星期二）	台灣桃園機場-新加坡樟宜機場
	新加坡國立大學計算機學院
12 月 17 日 （星期三）	亞洲台灣商會聯合總會青商會
	AWS 亞太總部
	駐新加坡代表官邸
12 月 18 日 （星期四）	CISCO 亞太總部
	新加坡個人資料保護委員會
12 月 19 日 （星期五）	新加坡樟宜機場-台灣桃園機場

二、新加坡國立大學計算機學院

新加坡國立大學計算機學院（NUS School of Computing，簡稱SoC），其起源可追溯至 1975 年在南洋理工大學成立的計算機科學系，是該地區歷史最悠久的計算機學系之一。1980 年隨著新加坡國立大學成立為其一部分；1998 年正式成立計算機學院。致力於提供優質教育、進行高等研究、加強全球與區域協作，並滿足社會對 IT 專業人才及技術的需求。

師生規模擁有約 252 名教學人員、222 名研究人員，目前約有 6,335 名學生，以及超過 1,540 名研究生（包含 1,000 名碩士生與 540 名博士生）。在 2025 年 QS 世界大學排名（QS World University Rankings）排名中，其計算機學系與資訊系統學系位居全球第 4 名，在 2025 年泰晤士高等教育世界大學排名（Times Higher Education World University Rankings）世界大學排名中，計算機學系位居全球第 11 名，並被評為亞洲計算機學系排名第一的大學。

在研究領域與產業合作方面

1. 多元研究方向：學院在資料庫、多媒體、計算生物學、網路安全、人工智慧（機器人與機器學習）、金融科技及計算社會科學等領域具有長期的卓越表現。
2. 強大的產學連結：與 Google、Grab、Microsoft、Singtel 等國

際知名企業建立聯合研究實驗室或合作夥伴關係，致力於將研究成果轉化為實際影響力。

3. 創新型教育：提供多元化的本科途徑，包含海外學院（NUS Overseas Colleges）實習計劃，讓學生前往美國矽谷、德國慕尼黑、瑞士洛桑等地「新創企業」實習。

此次拜訪的張義謙（Chang Ee-Chien）副教授，同時為新加坡國家網路安全研發實驗室（National Cybersecurity R&D Laboratories）首席研究員，首先分享目前學術界與業界在資料隱私與雲端安全上的關鍵技術與趨勢。

接著說明在新加坡國家網路安全研發實驗室方面，由新加坡國立大學負責營運，支援國家級資安演練。關注在關鍵資訊基礎設施（Critical Information Infrastructure，CII），涉及核心業務運作，支持關鍵基礎設施持續營運所需之重要資訊系統的資安維護。

最後在產學合作方面，張副教授分享新加坡國立大學設有產業諮詢委員會（Industry Advisory Committee），成員包含公部門（如 CSA 新加坡網路安全局、IMDA 新加坡資通訊媒體發展局、國防部相關單位）及私部門（如 Sea Group、淡馬錫控股）。委員會提供市場需求建議（如增加資安或 AI 課程），確保教學內容與業界接軌；企業亦透過贊助研究經費與獎學金深化合作。

新加坡國立大學產業諮詢委員會

	
張副教授經驗分享	NUS 科技願景
	
電腦歷史介紹	訪問 NUS 合影留念

三、亞洲台灣商會聯合總會青商會

亞洲台灣商會聯合總會（Asia Taiwanese Chambers Of Commerce，ASTCC）成立於 1993 年，是亞洲地區最具影響力的台商組織之一，會員遍布日本、新加坡、泰國、越南及印尼等十餘個國家與地區。「青商會」（Junior Chapter，ASTCCYC）為該總會轄下專注於年輕世代傳承與創新的重要分支，其成員組成主要為亞洲各地深耕已久的台商企業第二代，或是在亞洲各國創業的台灣青年，領域涵蓋科技、電商、服務業等。

青商會林奕丞會長 Bruno Lin 建議透過與民間性質較強的資訊及通訊科技等協會簽署 MOU，涵蓋面廣且政治敏感度低，且合作議題不侷限於單一產業，建議以「智慧城市」為大架構，將資安（Cybersecurity）、人工智慧 AI、物聯網（IoT）及通訊等不同面向納入，便於各類廠商與單位參與。

在資安防詐與公共安全科技方面，林會長介紹新加坡內政科技局（Home Team Science and Technology Agency，簡稱 HTX），是新加坡內政部成立的法定機構，專責「公共安全」相關科技研發，HTX 旗下設有 Hatch 創新中心，徵選全球新創團隊，提供資金（約 3 至 4 萬新幣）進行 POC（概念驗證）。專注於執法、監控、數據分析等「非商用」但「極具治理價值」的公共安全相關的科技。

林會長作為青商會領導者，同時具備新加坡在地深厚的政商網絡。青商會不僅是台商在亞洲的聯誼網絡，更是台灣「數位外交」與「智慧城市輸出」的關鍵中介節點。透過青商會其在地商業實力，協助台灣政府與當地私部門、科技協會建立實質合作。

	
拜訪青商會討論交流模式	與青商會林會長合影留念
	
青商會所在辦公大樓	青商會辦公室願眺濱海灣

四、Amazon Web Services（AWS）亞太總部

AWS 是全球雲端運算的領導者，其在亞太地區（Asia Pacific & Japan，APJ）的營運總部設於新加坡。新加坡不僅是 AWS 進軍亞太市場的首個據點，也是該區域最重要的戰略樞紐，負責統籌包括東南亞、紐澳、日本、韓國及大中華區在內的業務發展與技術支援。

掌管 AWS 亞太暨日本區公部門策略業務銷售與服務（APJ PS Head of Strategic Sales）的主管 Jaspal Johl 指出 AWS 亞太總部具備以下關鍵特點：

(一) 亞太雲端基礎設施的核心：AWS 於 2010 年在新加坡推出了亞太地區第一個「區域（Region）」，即 ap-southeast-1，這使得新加坡成為亞太區資料傳輸、低延遲連線以及資料中心運維的重鎮。對於追求資料主權與高可用性的政府客戶而言，這裡是亞太區最重要的技術心臟。

(二) 推動「智慧國（Smart Nation）」的關鍵夥伴： AWS 亞太總部與新加坡政府有著極為深度的合作關係，深度參與了新加坡「智慧國」計畫的基礎建設。從數位身分認證（Singpass）、數位政府服務到公共數據上雲，AWS 提供了底層架構與資安合規的解決方案。這也是為何各國政府頻繁前往新加坡總部考察的主因，旨在學習其如何協助公部

門在兼顧資安的前提下實現數位轉型。

(三) 公部門業務決策中心：設於新加坡的亞太總部擁有專門服務政府、教育與非營利組織的「公部門團隊（Public Sector Team）」。該團隊匯聚了專精於政府合規（如 ISO、GDPR）、資安架構（如零信任模型）以及數位政策的專家，負責協助亞太各國政府解決法規落地、資料在地化以及跨境傳輸等複雜議題。

拜訪 AWS 亞太總部 Jaspal Johl(中)與 Thong Seng Foo(右 1)

接著 AWS 亞太暨日本區公部門-政府客戶產業實務應用講師介紹在資料保存管理核心方面，AWS 有其獨家的 Nitro System 技術，技術特點 Nitro Cards 將虛擬機監控程序（Hypervisor）輕量化並硬體化，實現了系統級的物理隔離，摒除了管理人員存取權限。意味著即使是 AWS 的內部員工，也無法從底層存取客戶的資料。這是對政府機關資料上雲的重要信心基礎，確保資料主權與隱私的絕對性。

AWS Nitro System 架構示意圖

面對日益複雜的資安威脅，傳統的邊界防護已不足夠。AWS 建議採用「永不信任，始終驗證（Never trust, always verify）」的零信任架構。無論存取請求來自內部網絡或外部，都必須經過身份驗證。AWS ZTAG（Zero Trust Accelerator for Government，政府零信任加速

器）是 AWS 為美國聯邦機構邁向零信任架構（ZTA）而設計的解決方案。它將 AWS 雲端基礎設施與資安合作夥伴的解決方案結合，強調持續身分驗證、自動化政策執行與網路隱形，以保護遠端工作與混合雲環境。

政府零信任加速器示意圖

最後 AWS 可提供完整的教育訓練資源，協助人員考取 AWS 相關證照。建立政府同仁的「雲端即戰力」，實現「自己了解、自己調配」，以提升對廠商的監督能力與系統規劃的自主性，而非完全依賴外部廠商。

此次交流不僅解決了市府對雲端資安的疑慮，更為未來的智慧城市建設確立了具體的技術路徑。

	
AWS 亞太創新中心	AWS 簡介其技術特點

五、拜訪駐新加坡代表

為加速臺中市智慧城市發展及深化 AI 在公務體系之應用，本次出訪新加坡特別拜會駐新加坡臺北代表處童振源大使。童大使曾任僑務委員會委員長、駐泰國代表等要職，專長為國際關係與區域經濟，長期觀察新加坡政經發展，並與星國政府互動密切。本次訪談旨在透過大使視角，深入瞭解新加坡數位轉型的核心成功關鍵，尋求雙方未來更務實的合作與對接模式。

童大使表示新加坡政府高度重視數位經濟發展，依據星方數據，從 2018 年至 2024 年，新加坡數位經濟的年均複合成長率達 12%。目前數位經濟產值與重要性已超越傳統金融業，顯示新加坡已從金融中心成功轉型為數位創新樞紐。

首先，不同於部分國家僅停留於技術研討，新加坡的 AI 戰略具有極強的「實用主義」色彩，明確劃定交通、市政、醫療、教育與邊境管理五大領域，透過產官學協作推動 AI 普及，並設定 2030 年建構「智慧國家」的願景。2024 年，Tortoise Global AI 指數將新加坡列為全球第三，僅次於美國與中國。(註)

其次，政府推動「帶問題來解決」的培訓模式，例如利用 AI 處理稅務查詢、自動化內部公文撰寫、會議紀錄，提升行政效率，而非單純學習理論。

接著，新加坡政府科技局（GovTech）具備強大的軟體自主開發能力，其開發邏輯為「Whole-of-Government Approach」（整體政府途徑）。擁有大量工程師，親自開發如 Singpass 等核心應用。開發之初即考量跨部會通用性，避免資料孤島（Data Silos），實現「一處開發，全政府通用」。

第四，新加坡公務體系的高效能，源於其獨特的人才政策，新加坡的「官民交流」制度，新加坡有 1/3 的高階文官（副常長、司局長級）會借調到私人企業工作 1 至 2 年，確保政府官員了解民間技術與需求，並由政府補貼薪資差額，政府提供具競爭力的薪資待遇，確保一流人才留在體制內服務。

註：

有志一「童」》新加坡 AI 戰略藍圖 七大支柱構築亞太樞紐

https://talk.ltn.com.tw/article/breakingnews/5172069

拜訪童振源大使(前排中)，並與世界華人工商婦女企管協會新加坡分會會長尤妮(前排左 2)、當地星謠團體合影留念

林谷隆局長致贈台中水梨給童振源大使(右)

六、CISCO 亞太總部

Cisco 亞太總部不僅是該公司在亞太地區的戰略營運樞紐，更被打造為一座結合前瞻科技與永續理念的「活的實驗室（Living Lab）」。該總部整合了世界級的「客戶體驗中心（Customer Experience Center）」與「共創中心（Co-Innovation Center）」，展示了從網路基礎建設、資安防禦到混合辦公的最新解決方案。

作為支援新加坡「智慧國」願景的重要推手，該總部本身即是智慧建築的典範，佈建了數千個感測器，利用 Cisco 自身的網路技術即時監控能源消耗、空間佔用率與環境品質，完美體現了數位轉型如何落實於節能減碳與辦公效率的提升。此處不僅是技術展示場域，更是 Cisco 與政府、學術界及合作夥伴共同研發在地化 AI 與資安解決方案的創新孵化基地。

在 AI 時代，數據即國力，各國政府正積極推動「主權 AI」，旨在確保國家能掌握 AI 基礎設施的控制權，並利用本地數據培育在地人才與產業生態系。

為了滿足總總需求與創新，CISCO 提出以下解決方案。

(一)基礎設施轉型—從「集中」走向「分散」

隨著 AI 模型從簡單的對話機器人（Chatbot）演進為代理人（Agentic AI），運算需求呈現指數級成長。AI 流量成長了 46

倍，推論請求成長了 8-10 倍，形成了所謂的「Token 需求通膨」。傳統集中式資料中心正面臨電力、冷卻與空間的物理極限，已無法單獨負荷此類需求。Cisco 提出「分散式資料中心」架構作為解方。

1. 分散部署：將運算資源分散至不同地點（如邊緣運算中心），解決單一地點的能源瓶頸。
2. 光纖骨幹互連：透過高速光纖網路將分散的中心串接，形成邏輯上統一的運算聚落。
3. 統一管理平台：透過 Nexus Dashboard 等工具，實現跨中心的高效互連與統一可視性管理，簡化維運複雜度。

(二)AI 原生資安與數位韌性

1. 防禦典範轉移 Hypershield：傳統防火牆依賴網路邊界（Chokepoints）進行防禦，但在 AI 資料中心內，龐大的流量讓傳統架構產生盲點。Cisco 的 Hypershield 架構，這是一種 AI 原生的防禦機制，利用 eBPF（Extended Berkeley Packet Filter）技術，將資安政策直接植入伺服器作業系統核心，無需修改應用程式。
2. 預測性維運 Cisco Data Fabric：面對日益複雜的 IT/OT 環境，傳統的監控已不足夠。Cisco 展示了結合 Splunk 的 Data Fabric

架構，利用 AI 分析機器數據來預測潛在風險。

3. 對抗 AI 威脅深偽辨識（Deepfake Detection）：針對日益嚴重的詐騙威脅，Cisco 展示了整合 Pindrop 與 GetReal 的技術，能在視訊會議或通話中即時偵測「深偽」影像與聲音，保護政府與民眾的互動安全。

(三)智慧國的數位包容與未來工作場域

科技不應遺漏任何人，Cisco 展示了 Webex AI Assistant 的「即時語音轉譯（Speech-to-Speech Translation）」功能。這不僅是文字翻譯，還能模擬說話者的語調，將英語即時轉為中文或其他語言，這對於新加坡多語言環境的國際交流與住民服務上極具應用潛力。

Cisco 強調「連結的智慧（Connected Intelligence）」，透過 AI 輔助（如自動會議摘要、任務指派），提升人員的生產力。同時，Cisco 透過網路學院協助培育在地 AI 人才，解決技術缺口。

隨著人工智慧（AI）技術的爆炸性成長，政府與企業正面臨前所未有的基礎設施壓力與資安挑戰。本次參訪新加坡 Cisco 亞太總部，旨在了解新加坡作為「智慧國」的成功典範，如何透過公私協力模式，構建具備「數位韌性（Digital Resilience）」與「數位包容（Digital Inclusion）」的國家級 AI 基礎建設。

與思科全球數位影響力發展辦公室亞太區總監 Clarence Barboza（左 2）和金融暨工商事業群總經理盧佳成（右 2）合影留念

	
Cisco IOT 儀表板	IOT 整合視訊會議設備，牆面的鏡頭可自動偵測說話的人，並切換視視訊畫面

七、新加坡個人資料保護委員會

新加坡《個人資料保護法》（Personal Data Protection Act，PDPA）於 2012 年制定，並於 2013 年 1 月 2 日成立個人資料保護委員會（Personal Data Protection Commission，PDPC），專責管理及執行 PDPA。

PDPA 規範新加坡境內個人資料之蒐集、使用、揭露及保護，防止個人資料遭不當利用，同時亦有助於鞏固新加坡作為企業及跨國資料流動可信賴樞紐之地位。其適用範圍涵蓋以電子及非電子形式（包含紙本）儲存之個人資料。PDPC 之核心目標，在於保護個人資料與滿足機構基於合法目的使用資料之需求間，取得適當平衡。

PDPC 實際編制人員約 40 人，另由資訊通信媒體發展局（Infocomm Media Development Authority， IMDA）提供支援資源，合計約 80 人投入相關工作，整體採精簡人力、跨機關支援之運作模式，主要職掌如下：

(一)執行 PDPA

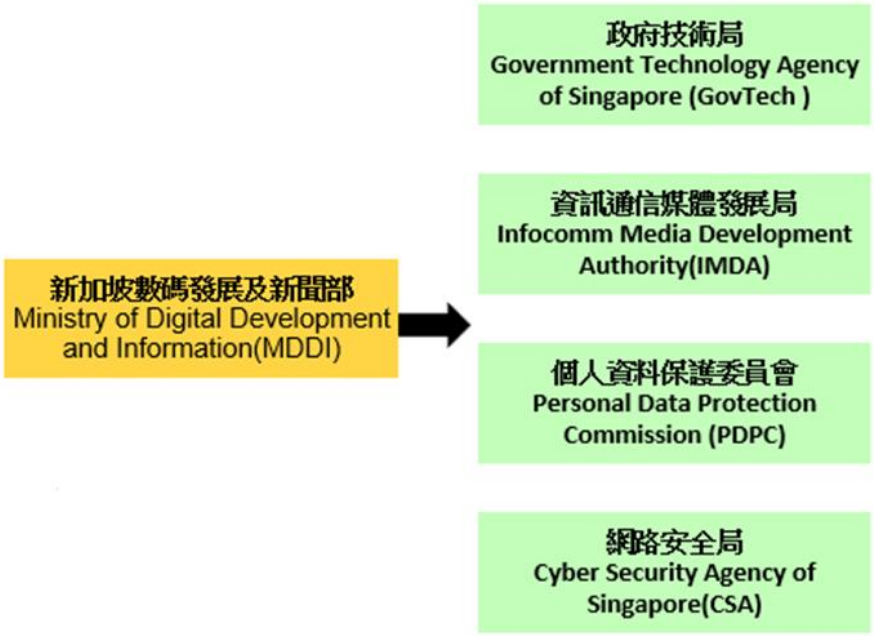
制定相關政策及諮詢指引，審查機構資料保護實務，必要時發布合規決定或改善指示，並與各產業監管機關合作共同監督合規情形。

(二)教育與推廣

制定相關政策及諮詢指引，審查機構資料保護實務，必要時發布合規決定或改善指示，並與各產業監管機關合作共同監督合規情形。

(三)請勿來電（Do Not Call，DNC）登記制度管理

監管「請勿來電」登記冊，確保民眾僅接收其同意之行銷訊息。



新加坡 PDPC 與其上級、平行單位架構圖

新加坡政府在個資的處理與推動方面有以下特點：

(一)企業責任及資料保護官制度

新加坡規定，所有公司不論規模大小，均須落實個人資料管理責任，PDPC 亦提供企業及資料保護官多項支援措施，包括最新政策資訊、免費研討活動及資料外洩趨勢分析等。

1. 資料保護官（Data Protection Officer，DPO）：可為專任人員，亦可由現有員工兼任。
2. 建立個人資料清冊：完整盤點組織所持有之個人資料，並記錄資料自蒐集至處置之生命週期。
3. 實施資料保護流程：由 DPO 檢視並確保組織實務符合 PDPA 規定。

(二)跨境資料傳輸與合規機制

新加坡對資料跨境傳輸採取「輸出管制」原則，資料輸入限制相對較少，但資料輸出時須符合 PDPA 規定。為促進經濟發展，新加坡透過示範合約等方式，協助企業確保資料接收方具備相當之保護措施，以簡化遵循流程。

(三)執法與裁罰制度

新加坡政府未針對守法良好之企業設置獎勵措施，但對違反 PDPA 之行為採取嚴格裁罰。2020 年修法前，所有組織最高罰鍰為 100 萬新幣；修法後，得依企業規模調整，最高可處以該企業於新加坡年度營業額 10%之罰款。

(四)公眾教育與中小企業輔導

PDPC 負責政策層級之教育與宣導，實務訓練多由培訓機構或合作單位執行，包括完整之 DPO 培訓體系。另 IMDA 亦透過社區

活動推動數位素養教育，協助民眾在理解風險的同時，安全有效地運用數位科技。

(五)新興科技治理經驗

新加坡 PDPA 採較原則性規範，對特定領域則以指引補充。在新興科技領域，如生成式 AI，仍以 PDPA 作為基本規範，確保個人資料於蒐集、使用及揭露過程中受到妥善保護，同時兼顧科技創新與資料合理利用。

對於特定技術或應用情境，則以發布指引方式，補充法條之適用原則。2018 年曾發生政府資助醫院遭網路攻擊導致個資外洩事件，該事件亦加速《網路安全法》相關措施之落實，顯示重大事件有助於凝聚社會共識並推動政策執行。

伍、心得

本次新加坡考察行程緊湊且充實，從學術前沿、產業實務到政府治理策略，全方位地剖析了新加坡邁向「智慧國」的成功方程式，與取經在資安防護、個資保護及生成式 AI 風險管理的最新實務，彙整以下心得：

一、 「實用主義」導向的 AI 戰略與全政府協作模式

此行體認到新加坡數位轉型的成功，不僅是技術的引進，更在於「體制之彈性」與「務實之精神」。新加坡的 AI 戰略不流於空泛的口號，而是明確劃定交通、市政、醫療等五大領域，推動「帶問題來解決」的培訓模式，讓公務員利用 AI 解決實際行政痛點（如公文撰寫、稅務查詢）。考量跨部會通用性，有效打破資料孤島。

二、 資安典範轉移：從「邊界防護」邁向「零信任」與「物理隔離」

我們見證了資安防護思維的巨大轉變。面對 AI 時代龐大的算力需求與複雜威脅，AWS 推動的「政府零信任加速器（ZTAG）」強調「永不信任，始終驗證」，確保無論內外網的存取皆須經過嚴格驗證。Cisco 的 Hypershield 技術則展示了

「AI 原生資安」的未來，利用 eBPF 技術將資安政策直接植入作業系統核心。這些技術展示告訴我們，資安不應只是外掛的配備，而必須內化為基礎設施的一部分。

三、 數據隱私與治理的平衡

在 NUS 計算機學院的交流中，張義謙副教授分享的「差分隱私（Differential Privacy）」觀點令人印象深刻。在公部門開放數據（Open Data）的過程中，透過在數據中加入雜訊，既能保留整體分析價值，又能確保個人隱私不外洩。此外，「機密運算」技術解決了雲端運算中的信任問題，確保數據在「運算中」也能受到保護，這對於處理市民敏感資料尤為關鍵。

四、 基礎設施的韌性與預測性維運

Cisco 指出，隨著 AI 流量成長 46 倍，傳統集中式資料中心正面臨物理極限，未來必須走向「分散式資料中心」架構。這對於臺中市規劃未來的運算資源配置提供了新思路。更重要的是，從「救火」轉向「預防」的維運思維，將能大幅提升數位服務的穩定性與韌性，降低突發事故對市民的影響。

五、 數位包容與防詐科技的社會責任

科技的進步不能遺漏任何人，Cisco 展示的即時語音轉譯技術，能協助克服多語言環境的溝通障礙，這對於服務新住民及

推動國際化交流極具應用潛力。而在防詐方面，針對日益猖獗的 AI 深偽詐騙（Deepfake），Cisco 整合 Pindrop 與 GetReal 的即時偵測技術，能在通話中即時辨識偽造聲音與影像。

六、 公私協力與人才流動的生態系

新加坡的成功，很大程度上歸功於其靈活的人才政策。從 NUS 產業諮詢委員會納入公私部門領袖以確保課程接軌市場，到政府高階文官與私人企業的「借調交流」制度，都顯示了新加坡致力於打破公私部門的藩籬。透過亞洲台灣商會聯合總會青商會的觀點，我們也了解到透過民間組織進行「數位外交」的靈活性與重要性。這些軟實力與生態系的營造，是支撐硬體建設永續運作的關鍵。

七、 新加坡與台灣於推動個人資料保護政策上，主要差異如下：

面向	新加坡	台灣（修法後）
立法取向	商業彈性導向	人權／隱私權導向
適用對象	非公務機關 PS.公務機關遵循公共部門資料共享與授權法，及資訊通信技術與系統安全管理指南約束	公務及非公務機關
主管機關	PDPC	PDPC（籌備處）
個資保護長	法規要求非公務機關皆	法規要求公務機關須指

	須設置	派個人資料保護長
跨境資料傳輸	對輸出有管制	對輸出有管制
罰則	最高可達營業額 10%	金額固定上限（2 億）
裁罰者	PDPC	PDPC

陸、建議

綜合本次考察之發現與心得，針對臺中市未來在智慧城市發展、資安治理等方面，提出以下建議：

一、 深化數據治理，落實隱私保護技術應用

參酌新加坡國立大學計算機學院學術觀點，建議在推動數據分析與資料開放時，研議導入「差分隱私（Differential Privacy）」技術，在確保個人隱私不被反推的前提下，最大化數據加值應用的效益。

二、 導入「零信任架構」與自動化合規機制，強化雲端資安

建議可參考 AWS 與 Cisco 之實務經驗，逐步將關鍵資訊系統之防護架構由傳統邊界防護轉型為「零信任架構（Zero Trust Architecture）」，落實身分持續驗證機制。針對機敏資料上雲，應評估採用具備物理隔離特性（如 Nitro System）之雲端服務，確保資料主權。此外，應善用雲端大廠提供之自動化合規工具，以取代人工檢核，降低同仁負擔並提升效率。

三、 建構 AI 驅動的數位防詐與預測性維運體系

面對生成式 AI 帶來的深偽詐騙威脅，未來如有相關影音運用，建議需同步評估引進即時深偽偵測技術（Deepfake

Detection），以提升市民數位互動之安全性。

四、 借鏡星國經驗，完善個資治理體制

個資法修法後，中央政府成立個人資料保護委員會為必然趨勢，參考新加坡經驗，法律制度能否有效落實，關鍵不僅在於法規本身，亦有賴完整之配套教育訓練、明確之權責分工及健全之組織運作機制。本府持續關注中央主管機關相關法令、指引及配套措施之發布進度，並適時檢視與調整地方配合措施，以強化本府個人資料保護業務之整體推動效能。