出國報告（出國類別：訪問）

2025VMware Explore 雪梨大會

服務機關： 內政部警政署刑事警察局

姓名職稱：
內政部警政署刑事警察局副局長陳世煌

派赴國家/地區：澳洲/雪梨
出國期間： 114 年 10 月 19 日至 10 月 25 日
報告日期： 114 年 11 月 21 日

摘要

本次研討會由 VMware 公司與 Broadcom 公司主辦，聚焦於澳洲及日本公共部門雲端架構、資安策略與數位轉型實務。隨著全球數位化加速，政府與公共機構面臨資料主權、資訊安全及混合雲部署的挑戰，各國積極探索如何在確保安全與合規的前提下，提升運算效率、降低成本並支持跨部門協作。

本研討會旨在分享 VMware 公司與 Broadcom 公司在公部門及企業的最佳實務案例、技術解決方案及策略規劃，協助公共部門建立可持續、可靠且高效的雲端治理體系，並介紹 VMware 雲端基礎平臺（VMware Cloud Foundation，VCF）及其功能模組的應用與實務。

在公部門 IT 現代化方面，研討內容涵蓋私有雲自動化、分散式資安、政府系統上雲、邊緣雲與分點治理、災難復原及智慧儲存整合。透過 VMware 雲端基礎平臺（VCF），政府可建置快速交付、標準化及可稽核的私有雲，結合自助服務平臺與 VCF 功能模組（如 GitOps、Azure VMware Solution、VCF Edge）實現自動化部署與跨地區備援，顯著縮短虛擬機與 AI 研發環境建置時間。分散式資安方案則強化零信任落實，透過微分段、入侵偵測與 AI 日誌分析，提升跨系統安全治理與政策部署效率。災難復原方面，透過 VMware Live Recovery（VMware 即時復原方案）提供快速切換、跨平臺資料回復及自動化 API（應用程式介面），滿足國防、警政及司法系統的高可用性需求；Pure Storage（智慧儲存方案）與 VCF 整合，則簡化混合雲資料管理、降低成本並提升效能。

企業端則透過 VCF 平臺整合計算、儲存、網路與管理功能，實現跨部門、多地區的私有雲治理標準化與資源共享。私有雲支撐核心業務，公共雲則應用於彈性場景，並結合 Private AI 平臺提供集中管理 GPU（圖形處理器）資源池、容器與虛擬機混合運算及多租戶治理。案例包括台積電、鴻海與中信金融業，展示 VCF 在大型組織落地過程中提升自動化運維、資源利用率與系統彈性的成效。

資安與跨區域防護亦為重點議題。透過零信任架構、網路分段、身份與存取

管理及日誌可視化，企業可有效防範資安威脅，並滿足多地區合規需求。Broadcom 強調未來企業雲端策略將偏向跨雲整合與混合部署，兼顧成本效益、彈性與資安防護，並透過自動化管理方案簡化跨資料中心操作，提升整體運營效率。

整體而言，研討會提供公共部門及企業雲端治理、資安及 AI 應用的策略指引與技術示範，呈現混合雲與私有雲結合、自動化運維與零信任架構的重要性，並透過實務案例展現跨區域協作、災難復原與資源最佳化管理的可行模式，對公共部門數位轉型及企業 AI 應用落地具有指標性參考價值。。

目　次

壹、 研討會的目的及背景

一、目的

隨著數位科技快速演進，政府機構與企業在資訊化與數位轉型過程中，面臨資料主權、資安防護、系統整合與雲端架構部署等多重挑戰。為提升公共部門雲端治理能力、保障資訊安全與支援跨部門協作，本次研討會由 VMware 公司與 Broadcom 公司主辦，旨在分享雲端現代化、資安防護及混合雲部署的最佳實務案例與技術解決方案。研討會希望透過案例示範與策略交流，協助公共部門理解私有雲、混合雲與邊緣運算的運作模式，掌握零信任架構落地方法，以及自動化運維與跨區域協作的實務做法。同時，研討會也關注企業端雲端部署與 AI 應用，分享如何在保障資安與合規的前提下，提高運算效率、降低成本，並支援多地區、多部門的資源共享與治理標準化。透過此次交流，與會者可獲取具體操作經驗與策略指引，為公共部門與企業在推動數位轉型與雲端現代化提供可行的參考模式。

此外，研討會亦旨在促進國際間知識與經驗的分享，尤其聚焦於澳洲與日本警政體系的實務案例，分析其在私有雲部署、災難復原、邊緣雲治理與資安策略上的成功經驗。透過這些經驗，與會者能理解如何在高度敏感與多元的公共服務環境中，建立可持續、可靠且高效的雲端治理體系。同時，研討會也強調跨區域協作、資料保護與資源最佳化管理的重要性，幫助公共部門及企業在數位轉型過程中降低風險，提升運營效率。

二、背景

全球數位化浪潮加速推動政府與企業資訊化轉型，各國公共部門積極探索雲端技術應用以提升行政效率、降低營運成本並加強資訊安全。然而，在推動雲端架構的同時，資料主權、系統安全性及跨平臺整合等議題成為亟需解決的挑戰。澳洲與日本在公共安全及警政管理領域的雲端應用，具有先進的治理模式及技術實務，可作為其他國家借鑑的範例。例如，澳洲警政與司法系統在私有雲與混合雲部署上，結合零信任安全策略、分散式資安管理及自動化運維，成功提升系統可靠性與跨部門協作效率；日本則在智慧資料分析、邊緣雲管理及災難復原規劃上，展現高度彈性與可持續的治理能力。

在企業端，隨著 AI 與數據分析的快速發展，跨部門及跨地區的資源共享需求逐漸增加。企業如何結合私有雲與公共雲，建立統一的資源管理、跨平臺運算與資安防護，成為提升競爭力的關鍵。VMware 公司與 Broadcom 公司具備在公部門及大型企業導入雲端架構、資安防護與

自動化運維的豐富經驗，因此透過本次研討會，分享其在台積電、鴻海及金融業等大型組織的實務案例，展現私有雲與混合雲結合、自動化管理與零信任架構落地的可行性。

綜合以上背景，本研討會提供公共部門與企業在雲端治理、資安防護及 AI 應用落地的策略指引，強調混合雲與私有雲結合、自動化運維及零信任安全的重要性，並透過實務案例呈現跨區域協作、災難復原及資源最佳化管理的模式，為數位轉型及雲端現代化提供具體參考與行動建議。

貳、 過程：公部門雲端現代化（Public Sector IT Modernisation）

（詳如附件 1，10 月 22 日下午議程簡報）

一、私有雲自動化：提升政府雲服務的「可消費性」

公部門過去普遍採用傳統虛擬化架構，多依賴人工操作，建置時間長且治理標準不一致。本次議程將 VCF Automation（VCF 自動化） 定位為政府打造「快速交付、標準化、可稽核」私有雲的核心技術。

VCF（VMware 雲端基礎平臺） 支援 Blueprint 與自助式服務平臺（Self-Service Portal），讓業務單位可自行申請虛擬機（VM）、人工智慧（AI）研發環境或測試平臺，大幅減輕 IT 管理負擔。透過 GitOps（以 Git 為中心的自動化運維模式），版本控制、系統設定與部署流程可一致化，避免人工失誤。會中特別示範 VM 與 AI 環境建置時間從 6－14 小時壓縮至約 20 分鐘，顯示自動化能大幅提升政府數位服務效率。

二、分散式資安：確保政府雲端環境的零信任落實度

資安威脅日益複雜，政府必須加強跨系統、一致的安全治理。本次議程介紹 vDefend（VMware 分散式資安套件） 如何透過 分散式防火牆（DFW）、入侵偵測（IDS） 與 入侵防禦（IPS） 構成微分段架構，使系統以最小權限與最小攻擊面運作。

VCF 可透過自動標籤與群組分類，使安全規則依「系統功能」與「資源角色」自動套用，而不再以 IP 管理，符合政府「系統多、環境複雜」特性。此外，Traceflow（網路封包追蹤與流量可視化工具） 協助快速定位異常流量，AI 分析工具可從大量日誌中提出動態防護建議，提升政策部署速度與精準度。

三、政府系統上雲：以 AVS（Azure VMware Solution）加速轉型

政府上雲常面臨歷史系統多、相依性複雜及高停機成本問題。本次議程指出 AVS 是適合政府的過渡方案，可保留 VMware 原架構並快速遷移至 Azure（微軟雲端平臺）。

AVS 支援零中斷遷移、跨地區備援與災難復原，確保業務不中斷。並可搭配 Azure 原生服務，例如 Log Analytics（Azure 日誌分析服務）、AI、資料倉儲等，使歷史系統「不重寫即可升級」，大幅降低轉型風險。

四、邊緣雲與分點治理：支援分散式政府服務的最佳架構

面對遍布各地的辦公室、分署與偏鄉場域，議程介紹 VCF Edge（VCF 邊緣雲），可將私有雲能力延伸至小型、分散的邊緣節點。

VCF Edge 支援單節點、小型叢集及 零接觸部署（Zero-touch Deployment），讓偏鄉也能快速啟用統一管理的 IT 服務。

以 Audi 全球工廠為例，透過邊緣雲集中控管多國工廠資料與生產環境，降低人力並提升一致性。政府若導入，可應用於邊境管理、交通、監控、執法等多種場域。

五、災難復原新標準：Live Recovery 強化政府韌性治理

政府資訊中心需面對自然災害、網路攻擊與重大事件，因此災難復原能力極為重要。本次介紹 VMware Live Recovery（VMware 即時復原方案），具十項核心升級，包括更快速的備援切換、應用層感知備份、跨平臺資料回復、版本快照與自動化 API。

這些功能提供政府單位更細緻的復原點（RPO，復原點目標）、更快的復原時間（RTO，復原時間目標），並可將備援流程標準化，適用於國防、警政、關務與司法系統的高可用性需求。

六、智慧儲存整合：跨雲資料管理更簡單

Pure Storage（純儲存） 與 VMware（威睿） 整合，強化政府在混合雲中的資料控管能力。透過 Pure1（純儲存雲端管理平臺）、Fusion（純儲存融合管理工具） 與 Cloud Block Store（CBS，雲端區塊存儲），政府可建立跨資料中心資料池，統一管理儲存資源，降低成本並提升 I/O（輸入/輸出） 效能。

此外，Pure Storage 已通過 VCF 9（VMware 雲端基礎平臺第 9 版）認證，意味系統整合可直接採用官方最佳化參數，降低設計與維運風險，確保混合雲環境下資料存取的可靠性與效率，同時提升跨區域資料共享與應用效能。

說明：講者介紹。

說明：議題簡報。

說明：全體參與者於活動場地集體合照。

說明：講者於投影幕前進行議題簡報。

說明：會議場地、舞臺與設備布置全景。

參、 過程：企業雲端整合的最新發展（詳如附件 2，10 月 22 日上午議程簡報）

一、私有雲治理架構的重整與標準化

自 Broadcom 公司收購 VMware 公司後，企業在私有雲治理上面臨新的挑戰與標準化需求。治理架構重整主要聚焦於以下核心議題：權限管理、租戶隔離、成本透明化與政策一致性。

過去，各部門在部署虛擬化資源時多自行制定操作規範，導致管理碎片化與資源浪費。在 VMware Explore 2025 研討會中，Broadcom 公司提出統一治理標準，使企業能透過集中化管理平臺，對不同部門的虛擬資源進行有效監控與稽核，並提升成本核算透明度。政策一致性亦讓多地區、多部門部署的企業雲端環境更易符合內部安全規範與外部法規要求。

此標準化治理不僅提升 IT （資訊科技，Information Technology）運營效率，也為資源分配與預算規劃提供明確指引，降低過度投資與重複建置風險。

二、VCF 架構在大型組織中的落地與挑戰（詳如附件 3，10 月 22 日重點分享簡報）

(一) 私有雲與核心數位轉型

過去五十年，資訊技術（IT，Information Technology）經歷多次轉型：從傳統 IT 基礎架構，到虛擬化（Virtualization）、軟體定義資料中心（Software Defined Data Center），再到雲端與人工智慧結合。

VMware 透過 Cloud Foundation（VCF）提供統一平臺，使企業能同時運行虛擬機（VMs）、容器（Kubernetes）及 AI 工作負載，實現「私有雲支撐核心業務、公共雲應用於彈性場景」的策略共識。

VCF 平臺涵蓋核心組件，包括 ESXi、vSphere、vSAN、NSX、vRealize Operations、Tanzu、SRM 等，整合運算、儲存、網路與管理功能，並結合 Private AI 架構，支持企業在自有資料與開放大模型上輕量投資實現 AI 應用。

(二) 大型企業落地案例

台積電：在晶圓廠部署 VCF（VMware 雲端基礎平台），建立 IT Cloud Zone（IT 資訊科技雲區）、FAB Prod/Dev Zone（晶圓廠生產/開發雲區）及 Bastion Zone（堡壘雲區），實現資源池化（將計算、儲存與網路資源集中整合以供多個系統彈性分配）、零信任策略（Zero Trust，所

有使用者與設備皆需驗證授權）、vMotion（虛擬機動態遷移技術）高可用性與自助服務功能。透過標準化擴展與自動化 VM 配置，提升資源利用率與 SLA（水準協議）水準，解決傳統 IT 資源分散、效能低與維運負擔重的問題。

中信金：運用 VCF（VMware 雲端基礎平台）整合資源，支持 GPU 運算、Kubernetes 容器（容器化應用管理平台）及 VM 混合工作負載。承載多個業務應用，包括反洗錢系統（AML）、智能徵審（AIGO）、AI 理專助理及網銀紅利系統，實現資源共享與自動化服務，降低運維成本並提升系統彈性。

鴻海集團：建構全球多雲架構（虎躍雲、龍華雲及印度、歐洲、越南、美洲雲），VCF（VMware 雲端基礎平台）支持多租戶（Multi-Tenant，不同使用者或部門共用同一雲平台但相互隔離）標準化部署、跨區域資源管理與統一管理策略，使全球業務能透過統一平台安全、靈活運行，支撐國際化生產與研發布局。

(三) 技術與運營挑戰

雖然 VCF（VMware 雲端基礎平台）提供統一私有雲平臺，但在大型組織落地仍面臨多項挑戰，包括資源整合與標準化：不同部門及應用系統需統一標準與管理策略，以避免 silo 化造成資源低效利用；安全與合規：跨雲、多租戶環境下，零信任架構（Zero Trust）及資料主權要求需同步落地；以及 AI 與容器運行：企業需決定哪些應用適合容器化，哪些使用虛擬機，並管理 AI/ML 運算與 GPU 資源調度。透過 VCF，企業可將傳統 IT 維運模式轉型為雲維運模型，實現運算資源池化（將計算、儲存與網路資源集中整合以供多個系統彈性分配）、網路安全管理與自動化運維監控，有效支援核心業務及創新應用。

說明：全體參與者於活動場地集體合照。

說明：講者於投影幕前進行議題簡報。

說明：講者於投影幕前進行議題簡報。

說明：講者於投影幕前進行議題簡報。

說明：講者於投影幕前進行議題簡報。

三、企業雲端整合的最新發展（詳如附件 4，10 月 23 日 AI case 分享簡報）

(一) 前言

隨著人工智慧（AI）與高效能運算（HPC）的迅速發展，企業在雲端整合與資源管理方面面臨日益複雜的挑戰。特別是對於擁有大量 GPU 運算需求的組織而言，如何有效管理算力、確保資料安全及降低 IT 投資成本，已成為雲端策略的重要核心。Broadcom 公司與 VMware 公司提供的 Private AI（私有人工智慧） 解決方案，正是針對這些挑戰所設計的完整企業平臺，透過集中管理、標準化資源以及多租戶治理架構，使企業能在安全、合規且高效的環境下運行 AI 應用。

(二) 背景與需求

過去，許多企業在 AI 專案推動過程中，會為每個開發單位分別購置 GPU 伺服器與相關基礎設施，造成資源利用率低下、管理複雜且成本高昂。例如，中華郵政透過小規模試驗逐步導入 AI，包括人臉辨識、金融詐欺檢測及生成式 AI 的 PoC 驗證（概念驗證），但若缺乏統一平臺，會增加運維與安全風險。類似地，全球知名 IC 設計公司在訓練與推理場景中，若僅使用少量 GPU，容易出現資源浪費與效能瓶頸。為解決

這些問題，企業亟需標準化、可擴充且安全的 Private AI 平臺。

(三) VMware Private AI 解決方案概述

VMware Private AI 建立於 VMware Cloud Foundation（VCF）與 Kubernetes（K8s）架構之上，提供統一的 GPU 資源池，使 AI 虛擬機（VM）與容器化微服務能夠同時運行。所有 GPU、VM 與容器資源皆集中管理與監控，方便管理者查看不同部門的使用情況，有效避免資源浪費。平臺採用標準化的軟硬體規格與自助式藍圖，自動化安裝 AI 開發工具，如 PyTorch、TensorFlow、CUDA 與 cuDNN，確保開發環境能快速部署，提升專案啟動效率。

此外，VMware Private AI 支援多租戶治理，透過命名空間（Namespace）隔離各部門的模型與資料存取權限，保障資料隱私與安全。平臺具備高效能 GPU 虛擬化能力，支援 NVIDIA H100 與 A100 GPU，同一張 GPU 可同時供多達 23 名使用者共享，實測效能接近裸機（bare-metal），滿足大型 AI 工作負載需求。開發人員可透過自助式介面選取所需 AI 工具環境，通常在 20 分鐘內完成整套開發環境部署，顯著提升開發效率並提供類公雲體驗。

(四) 安全與治理考量

Private AI 平臺的導入也解決了資料外洩與治理風險。例如，過去曾發生員工將半導體原始碼與會議錄音上傳至 ChatGPT，導致企業機密外洩。VMware Private AI 則提供企業專屬 AI 服務，所有數據在本地或私有雲環境運行，並可結合零信任網路技術進行隔離，降低潛在風險。此外，平臺還能透過真實資料避免 AI 生成虛假訊息（AI Hallucination），確保 AI 推論的可靠性。

(五) 案例分析：臺灣與國際企業

臺灣知名 IC 設計公司採用 vSphere vGPU 虛擬化技術，在訓練與推理場景中的效能接近裸機。透過 GPU 虛擬資源池化，企業能靈活調度資源，支援百張 GPU 的大規模部署，避免單點故障並提升高可用性（HA）。中華郵政則利用 Private AI 平臺進行人臉辨識、客服 AI 質檢及金融防詐應用，整合現有 GPU 資源池以提高利用率，同時保障資料安全。國際大型礦業企業運用 Private AI 平臺進行實時地質建模、礦車自動運輸及 OT 系統應用開發，顯著提升生產效率並降低安全事故風險。

(六) 效益與價值實現

導入 VMware Private AI 平臺後，企業可顯著提升 GPU 資源利用率，避免各專案分別採購設備，形成共享資源池以降低成本。開發效率也大幅加速，開發人員能快速部署 AI 環境，節省原本需要數週的手動準備時間。同時，多租戶隔離、零信任網路及企業專屬 AI 運行環境，強化資料安全與治理，保障敏感資料不外洩。平臺提供自動化與可視化管理功能，包括 GPU 成本計算、資源監控與使用報告，方便進行資本支出

（CapEx）與投資回報率（ROI）分析。更重要的是，統一平臺支援跨部門協作，使不同部門能平行運作 AI 專案，避免資源爭用與模型散落（Model Sprawl），提升企業整體 AI 運營效率。

四、雲端資安要求的強化與跨區域防護策略（詳如附件 5，10 月 23 日網路安全案例研究簡報）

(一) 資安挑戰與策略概述

隨著企業對雲端運算依賴日益增加，資安防護的要求亦隨之提升。Broadcom 在 VMware Explore 2025 中提出多項安全強化策略，涵蓋網路分段、零信任（Zero Trust，永不信任、始終驗證，每次存取皆需身份驗證與授權）、身份與存取管理（IAM，Identity and Access Management，控制使用者或設備存取資源的權限）、日誌可視化，以及跨區域合規策略，並結合 VMware Cloud Foundation（VCF，統一雲基礎平臺）與應用網路及資安（ANS，Application Networking and Security）技術，提供企業完整且自動化的安全解決方案。

(二) 零信任與全棧安全防護

透過網路分段，企業可將不同工作負載隔離，降低單一系統遭入侵後的風險擴散；零信任架構則確保每次存取都經身份驗證與權限檢查。VCF 結合 NSX（軟體定義網路平臺，提供微分段、防火牆、路由及 L2-L7 網路功能）與 vDefend 分散式防火牆（Distributed Firewall, DFW，保護虛擬化環境工作負載），提供從資料鏈路層（L2）到應用層（L7）的全棧網路安全，包括入侵偵測/防護（IDS/IPS，Intrusion Detection/Prevention System）、網路流量分析、資料外洩防護及零日威脅偵測，確保多租戶環境的資安穩健性。日誌與可視化功能提供完整操作追蹤，便於稽核與事件調查；Avi Load Balancer（應用層負載平衡器）則實現流量分配、自動 failover、SSL/TLS 卸載及 DDoS 緩解，進一步提升系統可用性與韌性。

(三) 跨區域合規與策略落地

跨區域部署的企業需考量地理法規差異，例如歐盟 GDPR（General Data Protection Regulation，通用資料保護條例）與亞洲地區個資保護法規。Broadcom 透過其資安工具與策略框架，協助企業在多地部署時維持統一的安全標準與跨區域資料治理（Cross-Region Data Governance），確保法規遵循（Geofencing Compliance）與安全一致性。

(四) 實務案例與效益

實務案例顯示，澳洲公部門及社會服務機構透過 VCF Automation 與 vDefend 分散式防火牆實現遠端安全連線、虛擬修補（Virtual Patching，針對無法立即更新的系統提供漏洞緩解）及多任務並行操作，即使在管理複雜的遺留系統與多平臺環境下，也能即時降低資安風險，保障關鍵

應用與資料安全。這些策略與技術不僅符合政府雲端安全要求，也為企業提供跨區域、高彈性、可擴展的雲端資安解決方案，強化整體韌性與合規能力。

五、跨雲運算與混合部署的未來路線圖

Broadcom 公司明確指出，未來的企業雲端策略將偏向跨雲整合與混合部署，兼顧成本效益、彈性與資安防護。企業將透過混合雲（Hybrid Cloud，結合私有雲與公有雲的運算模式，可實現資源最佳化配置）模式，將敏感工作負載留在私有雲（Private Cloud，企業自建或委外專用雲環境，用於關鍵與敏感工作負載），而較低敏感的應用則部署於公有雲（Public Cloud，第三方雲服務商提供的共享雲環境，適用於彈性、非敏感應用），以達到資源最佳化配置與成本控制。

在管理層面，LCA（Lifecycle Automation，生命週期自動化管理，用於自動化應用部署、資源調度及更新維護）與 ARIA（Application Resilience & Infrastructure Automation，應用韌性與基礎設施自動化管理，支援災難復原及跨資料中心操作）提供自動化的應用部署、資源調度與災難復原支援，使跨資料中心的操作更為簡便且可靠。Broadcom 同時提出多雲整合策略（Multi-Cloud Consolidation Strategy，集中於少數核心供應商與平台，以降低管理複雜度並確保資料同步與災難復原可靠性），指引企業在多雲環境中保持統一管理與安全標準。

整體而言，企業在規劃未來雲端策略時，需同時兼顧技術整合、運營效率、成本最佳化與資安防護。Broadcom 所提供的整合方案與管理工具，為企業進行混合雲與跨雲部署提供了清晰、可落地的藍圖，確保企業在擴展雲端應用與創新時，既能保持高效運營，又能維持安全與合規要求。

肆、 過程：Broadcom Sydney IC 設計中心與 AI 技術概況（詳如附件 6，10 月 23 日 IC 設計中心簡報）

一、Broadcom 全球布局與歷史

Broadcom Inc. 為全球半導體與通訊晶片領導廠商，其現行企業架構源自 Avago Technologies 於 2016 年併購 Broadcom Corporation 後整併而成。Broadcom 最初以寬頻通訊 IC 與網路晶片聞名，早期推動電信與寬頻市場成長，進入 2000 年代後，持續支援大型資料中心網通設備建置。併購後的 Broadcom 進一步拓展行動通訊、Wi-Fi、儲存控制器及高速互連技術，並投入人工智慧（AI）相關硬體與企業應用。其產品與技

術已成為支援全球 AI 資料中心與企業 AI 架構的重要基礎元件。

二、Sydney 設計中心角色與技術專長

位於澳洲雪梨的 Broadcom 設計中心隸屬半導體解決方案集團（SSG），整合類比、數位、系統與韌體相關的工程團隊，並與美國、印度、臺灣、以色列、希臘、荷蘭及新加坡等全球設計團隊協作。雪梨中心專注於高速互連、網路晶片、ASIC 子系統等設計領域，特別針對 AI 資料中心需求、低功耗處理、高速資料交換等技術進行優化。其在 CMOS 類比設計、數位訊號處理（DSP）與韌體控制方面具備深厚能量，能支援企業級 AI 與雲端基礎架構所需的關鍵元件開發。

三、AI 與 Wi-Fi 8 技術創新

Broadcom 積極投入下一世代無線技術，並參與 Wi-Fi 8（IEEE 802.11bn）標準制定，目前已提出前導架構與設計方案，主要面向終端裝置、家庭與企業無線網路應用。Wi-Fi 8 著重於提高資料傳輸速率、降低延遲、提升覆蓋與能效，並支援更多邊緣 AI（Edge AI）應用場景。除此之外，Broadcom 也透過自家高速互連、交換器晶片與資料中心網路方案，支援大型 AI 訓練與分散式運算架構，為企業 AI 服務與超級運算中心提供關鍵基礎技術。

四、戰略夥伴與全球合作

Broadcom 與全球主要晶圓代工廠與科技企業建立長期合作，例如台積電（TSMC）、Google、Meta 等，確保晶片供應與技術整合的穩定性。在 AI 資料中心領域，Broadcom 的高速網路交換器、NIC 與 PCIe/SerDes 技術被主要雲端服務商採用，並透過跨國協作持續支援超大規模資料中心與雲端運算環境的成長。透過多年度策略布局，Broadcom 已成為全球 AI、雲端與企業數位轉型的重要技術夥伴，並為警政雲端與政府資料中心的底層基礎設施提供關鍵支援能力。

伍、 過程：澳洲及日本警政雲端架構

一、前言

隨著全球數位化加速，公共部門在資訊管理、資料主權及雲端資安方面的需求日益提升，各國政府積極尋求最佳的 Hybrid Cloud（混合雲）與 On-Premise（本地部署） 平衡策略。

本研討會特別聚焦於如何透過 VMware Broadcom 的解決方案，實現公共安全、教育、衛生及交通等部門的雲端治理與自動化操作，並分

享澳洲及其他國家的實務案例與成功經驗。參與者涵蓋各級政府資訊長（CIOs）、技術顧問及資安專家，旨在提供策略性見解、操作性建議以及跨國合作機會，協助公共部門有效管理資安風險、提升運作效率，並確保資料合規性與本地化。

二、雲端架構講者介紹

(一) Josh Lambert：

任職於 VMware Broadcom 超過 11 年，現為亞太區及日本策略與顧問服務負責人，專長於大型組織的數位轉型規劃、商業策略與雲端架構設計。Josh 具備豐富的公共部門合作經驗，曾協助多個亞太地區政府推動雲端治理架構

(二) Jed Gerard：

現任 VMware Broadcom 澳洲政府與公共部門策略主管，專責推動澳洲各級政府採用安全且合規的雲端與網路技術。其主要工作包括協助公共安全、教育、衛生及交通單位導入 VMware 解決方案。

三、澳洲政府體系與警政架構概述

(一) 澳洲政府體系

澳洲採三層級政府制度，由聯邦、州與地方政府共同運作。聯邦政府負責國防、安全、外交、移民及跨州法律等全國性政策，並制定統一的資安、資料主權與雲端治理標準，以確保全國公共服務的一致性與安全性。各州政府（包括新南威爾士、維多利亞、昆士蘭等）主要負責具地域性特質的警政、交通、教育與衛生等業務，並依據各州需求發展獨立的數位化與資訊系統。地方政府則管理社區層級的基礎建設與公共服務，並在近年陸續推動智慧城市、資料治理與物聯網監測等創新方案，使地方行政更具效率與透明度。

(二) 澳洲警察體系

澳洲警察體系由聯邦與州層級共同組成。澳洲聯邦警察（AFP）負責跨國與全國範圍的重大犯罪，包括恐怖主義防制、網路犯罪、跨境毒品走私及國際警務合作，並設有資安與數位取證專責部門，支援全國在高科技犯罪上的偵查能力。州警察機關（如 NSW Police、Victoria Police 等）則負責地方治安、交通執法及刑案偵查，各州擁有獨立 IT 系統架構，但近年逐步朝向採用聯邦級資安標準，以提升跨州協作效率。警政單位在資訊化過程中面臨多項挑戰，包括偏遠地區網路連線品質不穩定、邊緣設備（Edge Devices）管理難度高、警用車輛行動化使資料同步與資安需求增加，以及需確保距離主資料中心千公里之外的警局仍能維持穩定運作。整體而言，澳洲警政資訊化需在廣大地理範圍、跨層級架構與公共安全需求間取得平衡。

四、澳洲政府的數位轉型重點

(一) 平衡本地與雲端環境（On-premise 與 Cloud）

澳洲政府早期大力推動「全面上雲（Full Cloud Adoption）」政策，希望透過雲端運算提升效能、降低硬體成本並加速跨機關資料共享。然而，隨著政策落地，逐漸發現並非所有工作負載（Workload）都適合放置於公有雲（Public Cloud），特別是涉及敏感資料（Sensitive Data）、高資安需求或具有法規限制（Regulatory Compliance）的系統，例如警政與國防領域的核心平台仍必須保留於地端（On-Premise），以確保資料主權（Data Sovereignty）及運作安全。

因此，政府逐步轉向更為務實的「混合雲（Hybrid Cloud）」策略，依照資料敏感度與系統屬性進行差異化部署：高敏感度資料與任務系統持續留在地端資料中心，以降低外洩風險、強化主權管理；而一般行政性或非敏感系統，包含電子郵件、公文管理與行政報表等，則部署於公有雲以提升擴充性並減少基礎建設維運負擔，也更能支援遠端工作（Remote Work）等彈性運作需求。

(二) 資安與主權（Cybersecurity & Sovereignty）

面對近年多起涉及國防、警政與公民個資的大型資料外洩事件（Data Breach），澳洲政府全面強化資安治理，並以 Essential Eight Framework（八大資安措施）作為所有機關必須遵循的核心標準。Essential Eight 涵蓋系統補丁管理、應用白名單、多重驗證（MFA）、存取控制（Access Control）、資料加密（Encryption）、備援策略、持續監控（Continuous Monitoring）與稽核（Audit & Logging）等面向，是政府資訊系統能否通過資安合規（Compliance）的最基本要求。

遵循 Essential Eight 不僅是技術層面的要求，更是文化面的轉變（Security Culture），透過明確規範提升公務體系的資安意識（Security Awareness），確保資訊環境在地緣政治、跨境數據流通與雲端遷移加速的情況下仍能維持安全、穩定並符合資料主權要求。

(三) 人工智慧（AI）應用與政策

澳洲政府近年積極推動人工智慧於行政流程的導入，包括試行 Microsoft Copilot 等 AI 輔助工具，用以提升文書處理效率、行政流程自動化與跨部門協作。然而，在推動 AI 的同時，政府亦高度重視 AI 安全（AI Safety）、倫理（Ethics）與隱私（Privacy）等議題，並建立多項治理原則。政府特別關注個資與隱私保護（Personal Data & Privacy Protection）、AI 模型透明度（Model Transparency）、決策可解釋性（Explainability）以及避免 AI 黑箱操作（Black Box Risk），確保公部門在導入 AI 時不會侵害民眾權益。

此外，針對警政體系可能使用的 AI 技術，如臉部辨識（Facial

Recognition）與犯罪預測（Crime Prediction），政府要求必須先進行倫理風險、偏誤（Bias）與社會影響（Societal Impact）評估，以確保 AI 應用在提升治安效率的同時，不會損害公平性、透明度與民眾信任。

(四) 可觀察性與成本管理（Observability & Cost Control）

澳洲政府在雲端治理上強調「可視化」（Visibility）與「可觀察性」（Observability），要求機關能即時掌握每項應用、虛擬機（VM）、伺服器（Server）及儲存資源的實際使用量與成本。透過整合式雲端儀表板（Cloud Dashboard），政府可同時監控硬體、軟體、能源與維運相關支出，使稅金使用更具透明度，也能有效提升跨部門決策品質。

這些儀表板提供多維度分析（Multi-Dimensional Analysis），協助管理者掌握年度預算變化、資源使用趨勢、能源效率（Energy Efficiency）與不同機關的成本分攤（Cost Allocation），進而推動更合理的資源配置（Resource Optimization）。可觀察性也支援災難復原（Disaster Recovery）、安全事件監控（Security Event Monitoring）及整體效能評估，形成政策導向的自動化治理（Policy-Driven Automation）基礎。

(五) 小結

整體而言，澳洲政府透過混合雲架構（Hybrid Cloud Architecture）、資安標準（Cybersecurity Standard）、AI 應用與可觀察性（Observability）建立完整雲端治理（Cloud Governance）策略，兼顧安全（Security）、成本（Cost）、效率（Efficiency）及資料主權（Data Sovereignty），為公共部門的數位轉型提供可複製的範例與操作指引。

五、VMware 公司與澳洲及日本警方合作案例

(一) 澳洲新南威爾斯州警察—在大規模下提升效率與韌性

1. 組織概況：

新南威爾斯州警察（New South Wales Police Force, NSWPF）管理規模龐大的 IT 環境，包含超過 5,000 部 x86 伺服器、約 15,000 至 20,000 名警員與 500 個警局網路節點。原四個資料中心合併為兩個，並另增一個公有雲實例，用於處理與儲存非敏感性資料。

2. 核心挑戰：

面對上述問題，NSWPF 與 VMware Broadcom 合作打造統一的私有雲平台（Private Cloud Platform），以強化敏感警務資料的安全性與資料主權管理，同時整合傳統與現代化應用至軟體定義基礎架構（Software-Defined Infrastructure, SDI）。其主要目標包括：確保關鍵系統達到全年 99.99% 的高可用性、藉由自動化與自助服務實現現代化 IT 運營模式、強化全棧可觀測性與成本控管，以及為未來 AI 與容器化架構奠定基礎。

導入後，NSWPF 在三年內展現明確的可量化效益。藉由資料中心整合與硬體效率提升，每年帶來約 1,190 萬澳幣的淨節省；透過 110 萬

次虛擬機即時遷移（vMotion），避免超過 9,000 小時的關鍵系統停機；並以 Site Recovery Manager（SRM）保護 324 項關鍵工作負載，顯著提升災難復原能力。自動化效益使每位管理員可維運 1,866 個虛擬機，同時藉由伺服器整合降低約 848 噸 CO_2 排放，兼顧效率與永續發展。

3. 未來路線圖：三階段整合雲之旅

展望未來，NSWPF 推動三階段私有雲發展路線圖。第一階段（至 2025 年底）以建置開發者就緒基礎（Developer-Ready Infrastructure）為核心，導入標準化平台、AIOps 與零信任微分段安全架構；第二階段（至 2026 年底）聚焦雲端與安全整合，建立自助式資源經紀人、統一 VM/容器管理與企業服務中心；第三階段（2027 年起）則將私有雲轉型為 AI 與 DevOps 的核心價值引擎，支援多雲管理、隔離式勒索軟體復原環境與面向民眾的 AI 服務。此路線圖展現 NSWPF 從提升效率到全面創新的持續進化方向，為警政數位轉型奠定長期且具韌性的基礎。

(二) 日本警察—從主機系統的安全優先遷移

1. 前言

日本警察廳的 IT 現代化是一場以「安全優先」為核心的長期轉型旅程，重點在於將高度客製化、維護負擔沉重的傳統主機系統（Legacy Mainframe Systems）逐步遷移至現代化私有雲平台（Private Cloud），並自專案起點即採用零信任架構（Zero-Trust Security）作為安全基礎。

2. 任務範疇與戰略驅動因素

日本警察廳肩負國家級任務，包括反恐、重大災害應變、跨區域調查協調與網路犯罪防治。此次轉型主要受到兩大戰略驅動因素促成：其一，日本政府明確要求國防、警政、衛生等關鍵部門，必須將核心資訊系統保留於內部環境，以強化國家安全與資料主權（Data Sovereignty）；其二，既有主機系統架構高度複雜、客製化程度極高，長期維運成本、開發成本與人力風險大幅上升，使轉移至更具彈性與可擴充性的架構成為必然選項。

3. 五年轉型時間表

在五年漸進式路線圖下，日本警察廳以 VMware Cloud Foundation（VCF）作為現代化私有雲基礎，分階段完成多項關鍵系統遷移。2020 年前，犯罪分析、調查支援與全國駕照資料庫仍依賴傳統主機；第一階段（約 2020 年）率先完成駕照系統遷移；第二階段（至 2023 財年）成功將調查與犯罪分析系統虛擬化，並大量導入 NSX 微分段（NSX Micro-Segmentation）及 Carbon Black 端點防護（Carbon Black Endpoint Protection），形成全面性的零信任防禦；當前進行中的第三階段則以全國公民身份平臺（National Citizen Identity Platform）遷移為核心目標，逐步建構完整虛擬化且高韌性的安全基礎設施。

展望未來，日本警察廳的重點將從「安全遷移」走向「智慧運營」。

一方面，計畫導入 AIOps（AI-Driven Operations），透過 AI 提升系統可觀測性、預測性維運與事件主動處理能力；另一方面，也正規劃建立隔離式勒索軟體復原環境（Isolated Ransomware Recovery Environment），確保在面對高端持續性威脅（APT）或跨系統攻擊時仍能維持任務連續性。

整體而言，日本警察廳透過高度安全導向的轉型策略，逐步完成主機系統現代化，並為後續 AI 應用、智能運營與高等資安防禦奠定堅實基礎，其案例也提供各國警政機關在規劃優先順序與技術路線時的重要參考。

說明：講者於投影幕前進行議題簡報。

說明：講者於投影幕前進行議題簡報。

說明：講者於投影幕前進行議題簡報。

說明：參與會議的與會人員聚精會神聆聽。

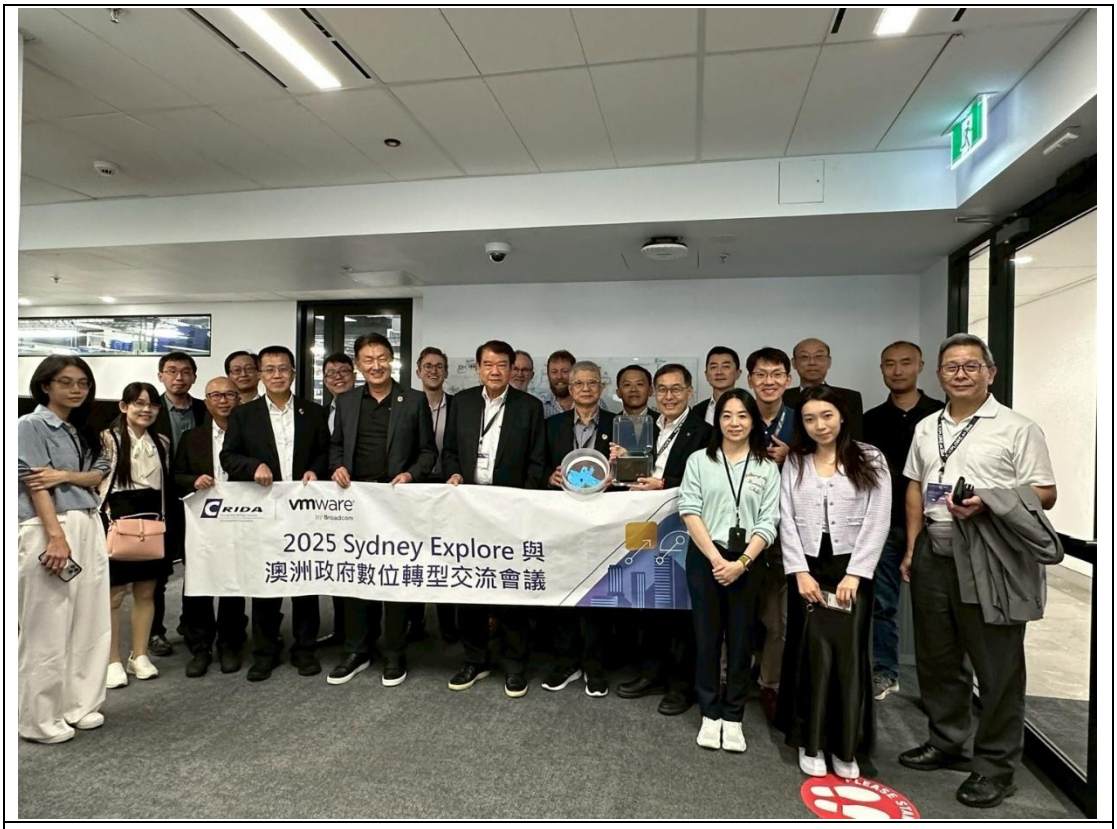
說明：講者與貴賓於會議現場合影。

說明：講者與貴賓於會議現場合影。

說明：講者與貴賓於會議現場合影。

說明：講者與貴賓於會議現場合影。

說明：會中與會人員向講者提問互動瞬間。



說明：全體參與者於活動場地集體合照。

陸、過程：警政 AI 應用案例：澳洲、新加坡與日本（詳如附件 7，10 月 23 日亞太地區警察 AI 運用簡報）

隨著人工智慧（AI）技術的快速發展，亞太地區警察機關積極導入生成式人工智慧（GenAI）及其他 AI 工具，以提升行政效率、支援前線執法及改善調查與情報分析能力。各國警察在行政營運、數位證據處理、訓練及犯罪預測等多個領域，已開始廣泛運用 AI 技術，形成各具特色的實務案例。本報告將以澳洲、新加坡與日本為例，分析其主要 AI 應用、面臨的挑戰與未來發展趨勢。

一、澳洲警察的主要 AI 應用

(一) 行政與營運效率

澳洲警察機關在行政與前線作業中逐步導入多項 AI 技術，以提升效率並降低人力負擔。生成式 AI 已能自動產生警察報告、證據摘要與其他文書草稿，並依據警員隨身攝影機錄音自動進行轉錄與整理。澳洲聯邦警察局（AFP）正評估導入此能力，以大幅降低行政成本，使警員能專注於前線勤務與案件調查。AI 也能協助快速整理案件卷宗、法律判例與跨單位資料，將大量資訊濃縮成重點摘要，對處理複雜案件尤其有利，並能縮短決策時

間。

在報案與調度支援方面，新南威爾斯州推動「BluLink」平臺，使 000 報案者可即時上傳影片、GPS 與其他媒體資料，為未來結合 GenAI 自動轉錄與事件分析奠定基礎。透過 AI 協助，調度中心能更快判斷事件緊急程度，精準派遣資源，提升救援效率與應變能力。

AI 亦被廣泛應用於警員訓練，結合擴增實境（AR）生成高度逼真的模擬環境，使警員能在安全條件下演練交通事故處理、暴力衝突及突發事件應變等情境，兼具成本效益與實務價值。

此外，AI 在心理健康支援上也發揮重要作用。透過預先摘要或模糊化處理血腥與衝擊性影像，減少警員長期暴露於高壓內容的頻率，降低職業壓力與創傷風險，提升警員心理韌性與整體工作效能。

(二) 數位證據與調查

在數位證據與調查領域，AI 技術大幅提升了警務單位的效率與精準度。透過 AI，監視影像、錄音檔、證人陳述及社群媒體內容能被快速整理，並生成事件、行動與互動的時間軸，使調查人員能迅速掌握案件脈絡。此外，AI 也可根據證人描述生成嫌疑人影像，類似法醫繪圖軟體功能，有助於加速案件偵辦。

部分警察單位已建立「數位證據雲」，整合多種資料來源，包括隨身攝影機與車載系統資料，AI 可分析並提高證據的關聯性與可用性，從而加速司法程序。同時，AI 可對犯罪報告與鑑識資料進行關聯分析，找出潛在模式與嫌疑人關聯，協助警方偵測過往未發現的關鍵線索。

更進一步，AI 可進行犯罪預測分析，預測犯罪發生的時間、地點與類型，協助警力與資源部署更加精準，提升預防犯罪的成效。這些技術應用不僅加快調查流程，也提高了警務運作的智慧化與策略性。

二、新加坡警察的主要 AI 應用

(一) 行政與前線效率

在行政與前線效率方面，新加坡警察透過 AI 技術大幅提升作業效能。AI 報案系統（R-COP）利用聊天機器人引導報案流程，自動生成報案草稿，減少警員文書負擔，特別在處理大量簡單案件時效率顯著提升。前線作業自動化則取代部分人工流程，使警力能重新部署至其他前線勤務或專案任務。此外，AI 結合機器人技術，可模擬海岸警衛及電擊槍訓練場景，降低訓練風險並提供可量化數據；社區互動機器人如 CODY 則與民眾互動，宣導防詐與治安資訊，增進社區安全意識與警民互信。

(二) 調查與情報應用

在調查與情報應用方面，AI 技術同樣發揮重要作用。透過與 INTERPOL 及本地機構合作，AI 可即時辨識深偽影像，有助防範詐騙及虛假資訊擴散。加密貨幣犯罪追蹤系統則協助警方掌握現代金融犯罪趨勢，提高偵辦能力。

先進影像分析技術結合可穿戴設備，可即時進行人臉識別與異常行為偵測，提升現場情報蒐集效率。AI 驅動的數位證據處理工具可快速提取、篩選並關聯各類證據，加快偵查進度並提升證據準確性，進一步強化調查與情報工作。

三、日本警察的主要 AI 應用

(一) 行政與偵查流程改進

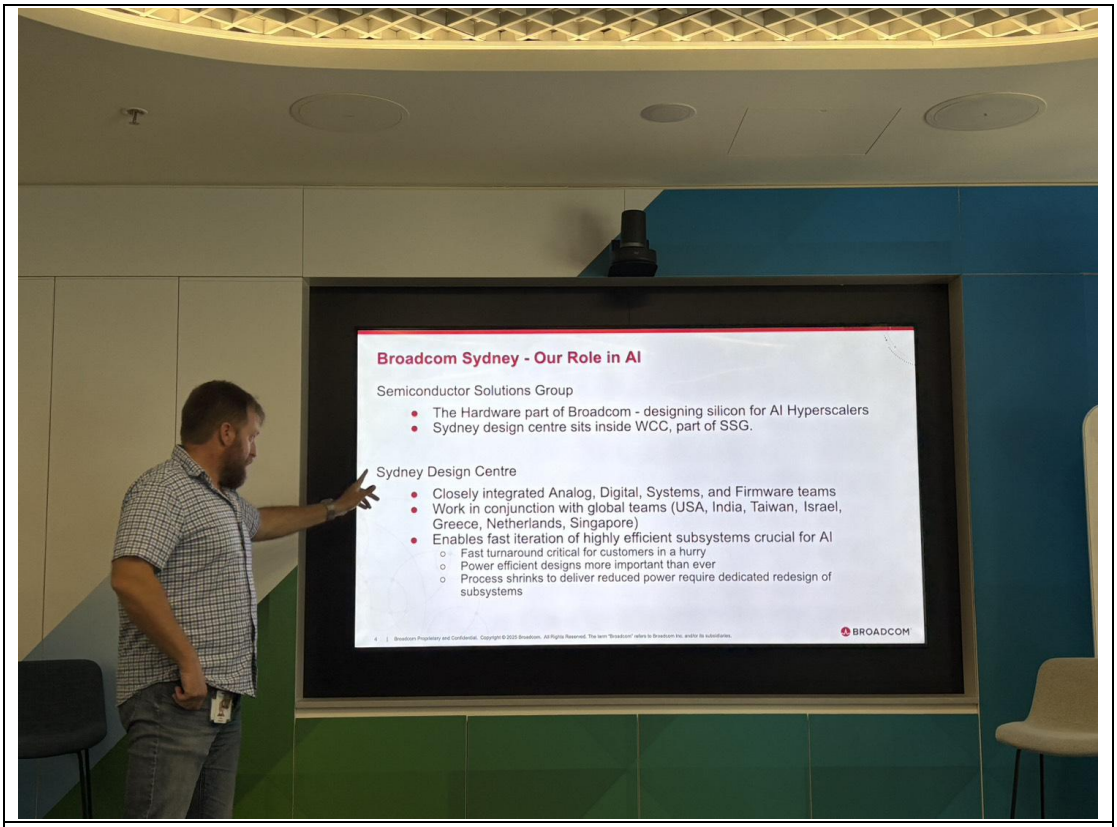
在行政與偵查流程改進方面，日本警察積極利用 AI 應對人口老化與勞動力不足帶來的人力挑戰。AI 被視為維持公共服務水準及提升警務效率的重要工具。專門的國家網路部門運用 AI 進行跨案件分析，辨識犯罪模式與潛在關聯，大幅提高分析速度與精準度，尤其適用於複雜的網路犯罪案件。此外，透過與私營企業合作開發 Crime Nabi 系統，促進犯罪預防與 AI 商業應用模型的整合，強化警民合作與資訊分享。同時，日本警察建立現代化且韌性的網路防禦架構，AI 作為核心工具，用於主動威脅偵測與防護。

(二) 調查與情報應用

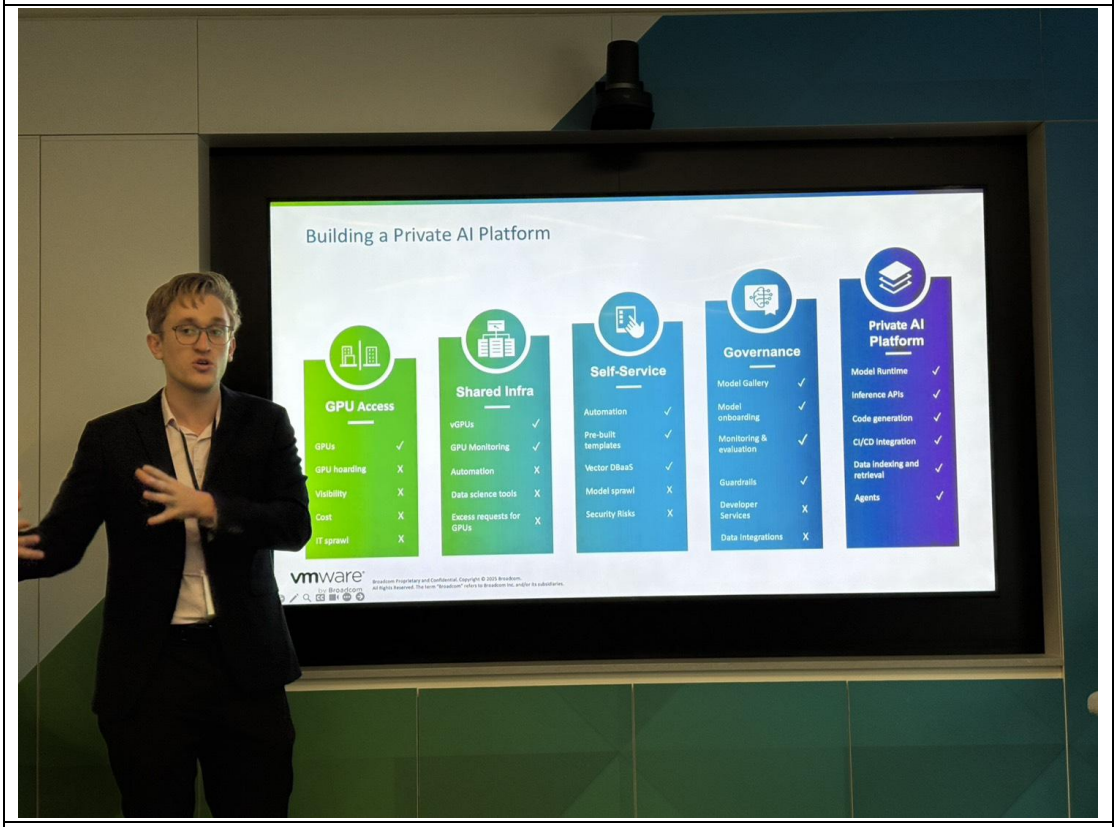
在調查與情報應用方面，Crime Nabi 系統可分析歷史犯罪、天氣與人流資料，建議最優巡邏路線，提升預防犯罪能力。AI 亦被應用於金融犯罪與詐騙偵測，分析百萬筆交易以識別可疑行為與犯罪集團核心人物，特別針對長者詐騙案件。此外，AI 可即時監控社群媒體威脅，標記或刪除可疑貼文，增強網路安全防護。數位證據分析工具則整合監視影像及其他來源資料，偵測潛在犯罪並識別可疑人物，有效提升調查效率與案件偵辦能力。

四、小結

綜合以上案例，亞太地區警察單位透過 AI 技術，不僅提升行政效率與前線作業效能，更強化數位證據處理、犯罪預測與跨部門合作能力。AI 已成為現代警務不可或缺的核心工具，對未來生成式 AI 在執法與公共安全領域的應用提供了實務範例。此外，隨著技術成熟，警政單位將能更精準調配資源、改善警員工作體驗、提升社會安全與公共信任。未來各國警察在 AI 應用上，仍需兼顧倫理、隱私保護及法規遵循，以確保科技進步與公共利益同步推進。



說明：講者於投影幕前進行議題簡報。



說明：講者於投影幕前進行議題簡報。

柒、心得與建議

總體而言，澳洲公共部門以「安全為核心、主權為基礎、效率為導向」推動雲端轉型，展現技術、法規與文化三方面的平衡。其成熟經驗提供我國警政單位寶貴參考，特別在雲端治理、資安標準化、AI 應用及跨部門協作等領域。若我國能結合本土需求，落實上述建議，將可大幅提升警政資訊基礎建設的穩定性、效率與國際競爭力，並逐步實現真正的數位韌性（Digital Resilience）。

一、建立符合本土需求的政府雲端資安標準：

澳洲在公共部門推動雲端與資訊安全治理時，採用「Essential Eight」作為統一標準，以確保資訊系統具備基本安全防護能力，包括補丁管理、權限控管、防惡意程式、備份與災難復原等八大面向。

對我國而言，可研擬「政府雲資安八項指標」，作為中央與地方政府雲端服務的統一資安框架。此標準應兼顧本土法律規範、資料主權要求以及警政單位的運作特性，特別針對敏感資料與公民個資的保護設計控制措施。標準化資安治理不僅能提升政府系統防護能力，也有助於跨部門協作，讓各單位在雲端環境中能快速評估風險、追蹤事件並採取一致的防護措施。此外，應建立定期稽核與評估機制，確保各項指標落實，並透過教育訓練提升使用者資安意識。透過這種方法，我國可以逐步提升政府雲端服務的安全成熟度，降低資安事件發生的機率，並保障公民資料安全。

二、推動跨部門共構資料中心，提升效率並降低成本

澳洲經驗顯示，透過共構資料中心與邏輯隔離方式，不僅能節省硬體與維護成本，也提升了系統整合與資源共享的效率。

對我國警政單位而言，可考慮跨部門共構資料中心，將硬體設備、儲存與網路資源整合管理，並利用邏輯隔離確保不同單位的資料安全與隱私。這種模式可減少重複投資，降低維護成本，同時為新技術導入（如虛擬化、私有雲、AI 分析系統）提供彈性基礎。建議在規劃共構資料中心時，先進行資源盤點與使用需求分析，並制定標準化操作流程與安全控管規範。此外，可導入即時監控儀表板，追蹤硬體使用率、網路流量與能耗情況，實現成本透明化與資源最佳化管理。長遠來看，跨部門共構資料中心不僅降低運營成本，還能提升整體資訊基礎建設的穩定性與可擴展性，為未來數位轉型提供有力支撐。

三、建置雲端成本與運營可視化管理機制

在澳洲，雲端運營的成本與資源使用透過即時可視化監控系統掌握，

使管理者能精準評估成本效益與資源分配效率。

對我國而言，建議建立雲端成本可視化儀表板，整合硬體、軟體、能源與維護等各項支出資訊，提供管理者即時數據支持決策。此舉能幫助各級單位了解不同系統或應用的成本結構，合理分配預算，並評估各種雲端部署策略（如混合雲或私有雲）的成本效益。此外，儀表板應可支援多維度分析，包括年度支出趨勢、各部門資源使用量以及能效評估，讓政策制定者和技術管理者能同步掌握整體運營狀況。結合預算管理與運營監控，還可進一步促進跨單位的透明協作，降低資源浪費，並為政策導向的自動化與智能化管理提供數據基礎。

四、導入 AI 輔助決策系統並強化倫理與法規監管

澳洲在公共部門導入 AI 系統時，特別重視倫理、透明度與數據保護，確保技術應用不違反公民權益。

對我國而言，建議先立法明確規範 AI 在警政及政府服務中的應用場景、資料使用原則與監督機制，確保技術部署符合法規與社會價值。AI 可應用於犯罪預測分析、案件輔助決策、資安威脅偵測與資源分配等領域，提高運作效率與決策品質。同時，需建立專門的倫理稽核機制，對 AI 系統的算法透明度、偏誤控制及結果可解釋性進行定期審查，避免技術濫用或歧視性決策。建議逐步導入 AI 輔助工具，先從低風險、非關鍵流程開始，累積經驗，再拓展至高敏感度或戰略性應用。透過法規保障與倫理稽核的雙重機制，可以在提升效率的同時維護公民信任，為未來數位轉型提供穩固基礎。

五、強化國際合作與政策導向的自動化推動

澳洲經驗顯示，面對人力不足與技術複雜性，自動化與政策導向的標準化流程是提升效率的重要手段。

對我國而言，應建立跨部門自動化策略，例如自動化資料備份、事件通報、系統維護與安全防護流程，減輕人力負荷，提升運營穩定性。同時，建議定期與澳洲、紐西蘭等具備成熟雲端與資安治理經驗的國家進行專家交流與技術研習，分享最佳實務與策略洞見，並結合本土法規與需求進行本地化調整。透過國際合作，我國警政單位可加速掌握新技術應用趨勢，提升跨境協作能力，並在資安防護、災難復原與數據治理方面達到國際標準。長期而言，結合政策導向自動化與國際經驗借鑑，將能有效提升警政資訊基礎建設的韌性、效率與可持續性，為未來智慧警務與數位政府轉型奠定堅實基礎。

捌、附錄

一、附件 **1**：**10** 月 **22** 日下午議程簡報，公部門雲端現代化（**Public Sector IT Modernisation**）。

二、附件 **2**：**10** 月 **22** 日上午議程簡報，企業雲端整合的最新發展。

三、附件 **3**：**10** 月 **22** 日重點分享簡報，**VCF** 架構在大型組織中的落地與挑戰。

四、附件 **4**：**10** 月 **23** 日 **AI case** 分享簡報，企業雲端整合的最新發展。

五、附件 **5**：**10** 月 **23** 日網路安全案例研究簡報，雲端資安要求的強化與跨區域防護策略。

六、附件 **6**：**10** 月 **23** 日 **IC** 設計中心簡報，**Broadcom Sydney IC** 設計中心與 **AI** 技術概況。

七、附件 **7**：**10** 月 **23** 日亞太地區警察 **AI** 運用簡報，警政 **AI** 應用案例。