

課程名稱：18506_企業私有雲資安風險與防護機制 課程摘要

本摘要由 Gemini AI 協助生成，僅供參考

1. 適合對象與能力門檻

- **適合族群：**IT/MIS 系統管理員、網路管理人員、資訊主管、企業架構師，以及需要評估私有雲/混合雲建置與資安防禦決策的企業管理者。
- **能力門檻：**普通。建議具備基礎的伺服器、網路網段（VLAN）與系統維運常識，課程將以實務經驗與案例分享如何選擇虛擬化架構與控制資安風險。

2. 課程核心大綱與架構圖

- **章節架構：**
 - **章節一：私有雲架構與實體/合規安全性** — 私有雲廣義定義與邊界、IDC 代管與企業自建比較、電力與網路雙迴路備援、實體門禁與安防。
 - **章節二：公有雲與混合雲架構安全比較** — 混合雲情境、SD-WAN 打通與資安 Policy 部署、情境與預算評估。
 - **章節三：虛擬化平臺選擇與管理主機防護** — 評估 VMware、Proxmox VE (PVE) 與 Hyper-V 運作特性與生態系、Console 控制臺隔離防護。
 - **章節四：網路存取控制與防護產品部署** — 內外網防火牆（UTM）、WAF 應用程式防火牆、內網流量監聽（NPartner/雲智維）與端點 EDR/MDR 監控、韌體與情境訂閱更新。
 - **章節五：儲存裝置（Storage / NAS）架構與備援** — 運算與儲存單元拆分（HA 高可用性）、Storage 與 NAS 使用情境差異與風險評估。
 - **章節六：常見駭客攻擊手法與私有雲防衛實務** — 剖析端點釣魚/社交工程、SQL Injection/API Token 攻擊、3389/遠端跳板入侵、DDoS、勒索病毒與資料防外洩加密。
 - **章節七：身份驗證、零信任與資安管理運維** — 多因素驗證

(MFA/SSO/Azure AD)、零信任架構存取控制、開源中央監控與 Log 收集工具 (LibreNMS / Graylog)、離線備份與 ISO 27001 風險識別。

3. 必備前置知識清單

- **基礎伺服器與虛擬化概念**：了解基本的實體 Server、VM (虛擬機器) 與系統維運常識。
- **基本網路基礎知識**：對 IP 地址、網段切分 (VLAN)、防火牆 (Firewall) 與 VPN 連線有基本概念。

4. 專有名詞與概念辭典

- **私有雲 (Private Cloud)**：企業專屬且資源 100%自主掌控的伺服器運算架構，可自建於公司機房或託管於 IDC 機房。
- **WAF (Web 應用程式防火牆)**：專門保護 Web Server 的防火牆，能防止惡意流量過濾，最基礎可勾選阻擋 SQL Injection (SQL 注入攻擊)。
- **EDR / MDR (端點偵測與回應 / 代管偵測與回應)**：安裝於 Server 或端點電腦上的安全監控軟體；MDR 則結合外部專家/AI 機制協助實時監控，當發現攻擊時可自動切斷網路隔離。
- **零信任架構 (Zero Trust)**：基於「不信任任何連線」原則，透過 VPN 鎖定來源 IP、SSL 憑證、多因素驗證 (MFA) 與最小許可權分割網段，進行多重檢查。

5. 課程學習職能對照

- **對應職能名稱**：雲端系統架構師 / 資訊安全維護工程師 / 系統管理員 (SysAdmin)
- **主要工作任務/能力指標**：
 - **雲端與虛擬化架構評估能力**：能根據企業預算與業務情境，規劃私有雲/混合雲建置方案，並選擇適當的虛擬化平臺 (VMware/PVE/Hyper-V) 與儲存設備 (Storage/NAS)。
 - **網路安全與存取控制規劃能力**：能劃分內外網段、隔離管理 Console，部署 WAF/內網防火牆/MDR 並設計零信任與多因素驗

證機制。

- **資安防護與災害復原執行能力：**能識別常見駭客攻擊（SQLi/勒索軟體/跳板入侵），落實軟體訂閱更新、離線備份與 RTO 復原順序規劃。