



從 NAS 到 AI

資訊安全與 AI 應用

資訊安全是守住公司的招牌，以及多年累積的設計資產
也是你能安心用 AI 的前提

| 講師簡介 | Speaker Profile



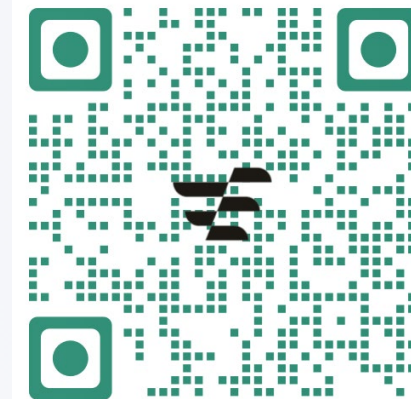
Lee Pan (潘冠中)

Backend / Infrastructure / 資訊安全 / 系統架構

專注於 AI、資訊安全與軟體開發的交叉領域，致力於打造智能化解決方案

- 緯創資通 (Wistron) | 技術主任
- 鴻海科技 (Foxconn) | 資深工程師
- 群創光電 (Innolux) | 資深工程師

聯絡我們：Lee_Pan@eagleai.tw / info@eagleai.tw



**built well.
billed right.**

eagle ai © 2026. all rights reserved.



01

第一部分 · 觀念篇

你保護的不只是資料
而是公司的營運

為什麼要做資安？資安不是目的，而是手段

Confidentiality 機密性

機密資訊未經授權情況下，外人無法取得、閱覽

CIA 資安鐵三角

Integrity 完整性

機密資訊未經授權情況下，
外人無法竄改、刪除

Availability 可用性

資訊不會因任何因素而中斷或
停止，隨時都處於可工作狀態

資料	最怕發生	預防方式
進行中的圖檔	打不開	備份、快照
請款、匯款、合約	被改、被冒充	二次確認、MFA
競圖、投標、個資	外流	權限、離職收回、地端 AI

- CIA 三要素沒有固定優先順序
 - 銀行重視完整性（帳務不能錯）
 - 醫院重視可用性（系統不能停）
 - 軍方重視機密性（資料不能洩）

勒索軟體 (Ransomware)



無法正常工作，團隊陷入空轉

並非被駭客針對

絕大多數是系統自動亂槍打鳥，防護較弱的越容易被攻擊

有備份 ≠ 安全

備份跟正本不應該放在同一個地方

停工的代價比贖金高

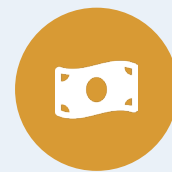
送審延誤、業主流失、團隊空轉

企業電子郵件入侵 (BEC, Business Email Compromise)



1. 潛伏

駭客潛進公司信箱，並觀察信件如何往來與什麼時候要請款



2. 動手

冒充你寄一封信給業主
「帳號換了，請改匯到新帳戶」



3. 匯出

業主不疑有他照做，錢一匯出去就進了詐騙帳戶

公司內最常見的錯誤

鬆散的制度漏洞，導致大門大開讓不肖人士有機可乘



手滑刪除 / 覆蓋

同仁不小心刪掉或用舊版覆蓋了整個專案資料夾



離職沒收權限

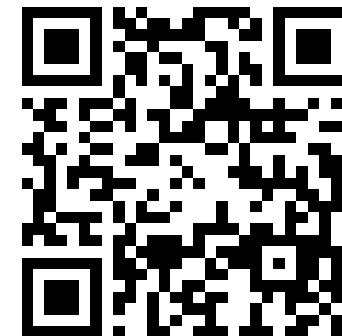
離職同仁的帳號沒關，依然能連進 NAS 與雲端



資料分享權限過大

分享出去的連結，實際上可以看到整個NAS的內容

每天都在發生的事



96%

勒索軟體的受害者
大多數是中小型組織

越小的單位越常被當作目標，因為
防護通常最弱

US\$3B

光是商業 email 詐騙就高
達 30 億美元

兩萬多件通報，平均一件超過 12 萬
美元

> 99%

帳號被盜
開啟 MFA 就能擋掉

免費且十分鐘內即可設定完成，防
護效益最高

臺灣近年的真實案例

年份	事件	發生什麼
2016	第一銀行 atm 盜領	潛入內網後，借合法的 ATM 更新管道遙控全臺 41 臺 ATM 吐鈔，盜走 8,327 萬元
2017	遠東銀行 swift 盜轉	入侵國際匯款系統，盜轉約 18 億元到海外三國
2018	台積電機台中毒	一個 SOP 疏忽讓蠕蟲病毒鑽進更新不全的產線，數小時內全臺晶圓廠大當機，損失逾 52 億元
2020	中油、台塑勒索軟體	加油站一度刷不了捷利卡、中油 Pay
2025	馬偕醫院勒索軟體	CrazyHunter 連攻 600 多臺電腦，急診一度癱瘓，1,660 萬筆病歷流入暗網

EBC、釣魚 email 詐騙



寄件地址怪怪的

網域少一個字母、大小寫混淆
例如 rn 假裝 m



製造急迫或機密

「今天內處理」、「別跟別人說」



連結與附件可疑

滑鼠移上去看真實網址；不明附件別開

本段小結

資料與資訊安全是為了要保護重要資產



工作能力

圖檔打得開，案子走得動



現金

付款詐騙防得住



信譽

業主的信任不流失



設計資產

多年心血不消失

02

第二部分 · 檢視篇

安全的公司會長什麼樣子？

資料有位置、帳號有主人、權限有邊界、備份可恢復、事發時有應變SOP

六個問題，快速健檢

1 資料

要找三年前某個案子的圖，你
5 分鐘內找得到嗎？

2 存取

最近一個離職的同事，你確定
他的帳號已經封鎖了嗎？

3 備份

若 NAS 今天突然故障，你是否
有另一份、親手還原過、確定
打得開的備份嗎？

4 帳號

有設定多道帳號安全驗證機制
嗎？

5 AI

哪些資料不能丟給 AI，公司有
一句大家都知道的規則嗎？

6 應變

你知道第一步做什麼、先打給
誰嗎？

中小企業基本資安防護指引

數位發展部資通安全署 · 115 年 4 月發布《中小企業基本資安防護指引》



帳號管理

管好公司的「鑰匙」：
密碼 15 個字元以上、不重複，
重要帳號一律開 MFA



設備與資料管理

顧好公司的「財產」：
開自動更新、照 3-2-1 備份、
把設備的預設密碼改掉



資安意識訓練

人要認得出釣魚信、
知道出事第一步找誰，
並善用 TWCERT/CC 等免費資源

資料夾結構

2026_A012_中正路李宅/

- |—— 00_專案管理/ 合約、報價、變更同意書、時程、會議紀錄
- |—— 01_業主往來/ 重要 email 存檔、LINE 重點截圖、確認紀錄
- |—— 02_基地與法規/ 地籍、都計、現勘照片、法規檢討
- |—— 03_設計/
 - | |—— 01_概念/
 - | |—— 02_基本設計/
 - | |—— 03_細部設計/
- |—— 04_送審/ 各階段送審圖、審查意見、補正
- |—— 05_施工圖/
- |—— 06_定稿/ 對外正式發出去的最終版本，只有這裡算數
- |—— 07_施工與監造/ 工地照片、監造紀錄、缺失改善
- |—— 08_請款與計價/ 請款單、計價表、發票
- |—— 09_外包與協力/ 結構、機電、景觀、透視圖
- |—— 99_過程稿/ 想留但不重要的東西，丟這裡

專案資料夾的命名

- 範例：年份_案號_案名
- 年份
 - 放最前面，電腦會自動排序
- 案號
 - 自行編碼，公司統一規則使用即可

專案底下固定分類的資料夾

- 範例：序號_類別
- 序號
 - 放最前面，電腦會自動排序
- 類別
 - 依使用需求增減

檔案命名 「案號_圖別或文件別_版次_日期」

- 範例

A012_結構_基礎配筋_v02_20260901.pdf

A012_合約_業主用印版_20260620.pdf

A012_會議紀錄_第三次業主會議_20260714.docx

A012_請款_第二期_20260830.pdf

- 不好的範例

A012_合約_最新版.pdf

A012_合約_最新版(2).pdf

A012_未命名.pdf

A012 合約 用印版 20260901.pdf

合約_用印版_20260901.pdf

其他常見地雷

- 不使用空格，改用底線 _
- 不使用這些特殊符號
 - / \ : * ? " < > |
- 需注意檔案名稱不要過長
 - 影響查看
 - 應考慮是否需要切分資料夾去存放
- 全形符號
- 日期格式混用
 - 20260901
 - 2026_09_01
 - 2026-09-01

備份的黃金法則 321

不是有備份就安全了，重點是如何存放



3 份資料

原檔 + 兩份備份



2 種不同媒介

雲端、外接硬碟、NAS、電腦...等



1 份異地

雲端、另一台電腦(未與公司網路相通)

發生事件	備份必須滿足
硬碟或NAS故障	要有第二份，且不在同一台機器上
被勒索病毒鎖住	異地備份
資料被覆蓋或誤刪	多版本備份



一句提醒

備份後的資料與檔案，需要驗證是否能正常還原

備份的常見的誤會

資料備份是任何資料管理策略的關鍵要素

錯誤認知	真正目的
RAID 就是備份	• RAID 是兩顆硬碟互相鏡射，預防的是「硬碟故障」 • 誤刪、存錯覆蓋、勒索軟體加密 • RAID 會把錯誤同步到兩顆硬碟上 • RAID 是為了不停機，不是為了救資料
同步就是備份	• Google Drive、OneDrive、Dropbox 的同步資料夾 • 這些是同步，不是備份 • 同步的意思是「讓兩邊長得一樣」 • 刪掉一個檔案時，雲端上也會被刪掉 • 勒索軟體加密檔案，雲端上也會被加密 • 同步是為了方便，不是為了救命
備份碟一直插著	• 備份用的外接硬碟長期插在電腦或 NAS 上，勒索軟體一樣看得到它，一樣會加密它 • 備份完就拔掉，拔掉的硬碟，任何軟體都碰不到

帳號與權限：不必要的共用帳號與密碼

- 檔案被刪除或變更，紀錄上都是同一組帳號
 - 無法確切得知是誰操作
- 有人離職，帳號無法關閉
 - 密碼要換嗎？
 - 換了就是全部有在使用的人都要重新去記新密碼，相關軟體也要一併更新
- 有人外洩帳號密碼，全公司一起遭殃
 - Credential Stuffing，當駭客取得帳號密碼後，透過自動化測試的方式，去嘗試各個系統與服務
- 權限沒辦法分層
 - 沒有辦法去區分每個人的權限
 - 大家都有權限看的到該帳號的所有資料

密碼規則

- 密碼長度比複雜度重要
 - 資安署的建議是 15 個字元以上
 - 不同服務不重複
 - 不使用容易聯想出規律的密碼
 - 隨機密碼產生器
 - <https://www.avast.com/zh-tw/random-password-generator#pc>
- 善用密碼管理器
 - Apple iCloud 密碼
 - Google 密碼管理工具
 - Bitwarden
 - 1Password



密碼管理器

每個網站不同的密碼，不需要硬背，也不需要寫在便利貼，把「記密碼」交給工具，人只要記一個主要密碼

多因素身分驗證 (MFA, Multi-factor authentication)

三種常見的 MFA 方式



簡訊驗證碼

有比沒有好，但有機率會被攔截



驗證 App

Google Authenticator
Microsoft Authenticator
免費且離線



實體安全金鑰

一個 USB / NFC 的鑰匙
適合最重要的帳號

哪些一定要開？

- 公司 email、雲端硬碟、網路銀行、密碼管理器
- email 排第一，因為所有其他服務的「忘記密碼」通常都會寄到註冊的 email 當中，若 email 被盜，相當於所有帳號都被盜

本段小結

「有安全」 = 這五件事你都答得出來

1

資料有位置

2

帳號有主人

3

權限有邊界

4

備份可恢復

5

事發時
有應變SOP

03

第三部分 · 行動篇

先做什麼？要花多少錢？

三階段資安防護

第一級・基本防護

帳號權限
MFA
備份機制

防火牆
訪客 Wi-Fi 隔離
專人定期巡檢

第二級・營運防護

第三級・成長與韌性

完整權限與資產管理制度
AI 與外部軟體使用政策

第一級：基本防護

第一級・基本防護

開啟 MFA 雙重驗證
使用企業版 email / 雲端服務
電腦與 NAS 系統定期更新修補
建立 NAS 以外的第二份備份
落實到職 / 離職帳號權限清單
制定基礎檔案與資料夾存取規範

第二級・營運防護

第三級・成長與韌性

第二級：營運防護

第一級・基本防護

開啟 MFA 雙重驗證
使用企業版 email / 雲端服務
電腦與 NAS 系統定期更新修補
建立 NAS 以外的第二份備份
落實到職 / 離職帳號權限清單
制定基礎檔案與資料夾存取規範

第二級・營運防護

訪客 Wi-Fi 與內網 VLAN 隔離
安排專人定期巡檢與維護
啟用安全遠端存取 (VPN)
定期清查系統帳號與離職人員
備份定期還原測試
年度教育與演練

第三級・成長與韌性

第三級：成長與韌性

第一級・基本防護

開啟 MFA 雙重驗證
使用企業版 email / 雲端服務
電腦與 NAS 系統定期更新修補
建立 NAS 以外的第二份備份
落實到職 / 離職帳號權限清單
制定基礎檔案與資料夾存取規範

第二級・營運防護

訪客 Wi-Fi 與內往 VLAN 隔離
安排專人定期巡檢與維護
啟用安全遠端存取 (VPN)
定期清查系統帳號與離職人員
備份定期還原測試
年度教育與演練

第三級・成長與韌性

建立元整權限與資產管理制度
訂定 AI 與外部軟體使用政策
定期執行釣魚信件演練
訂定資安事件應變流程
第三方軟體資安風險評估(TPRM)



先把第一級做完
就已經贏過八成

權威資安標準與合規體系 (SOC 2 & ISO)

資安標準	說明	目的
ISO 27001	目前全球最廣泛採用的資訊安全管理系統國際標準	證明我們有一套完全符合國際標準的資安管理規則
ISO 27017 / 27018	- 專門針對雲端環境 (27017) 與顧客個人資料防護 (27018) - 已納入 ISO 27001 稽核範圍	
SOC 2 Type 1 / Type 2	- Type 1：檢查你的制度寫得好不好 - Type 2：由第三方機構，在連續半年至一年的期間內，隨時間空並抽查	證明公司的安全是「365 天每天運作」，而不是「稽核那天演出來的」

其範疇覆蓋安全性、機密性及可用性

加密技術 (AES-256 & TLS v1.2)

資安標準	說明	目的
AES-256	- 靜態資料加密 - 銀行地下金庫與保險箱	就算有人把整個伺服器硬體偷走，沒有金鑰也完全解不開任何一張設計圖檔
TLS v1.2	- 傳輸中資料加密 - 全程武裝齊全的運鈔車與專用通道	上/下傳資料或跨國協作時，資料在網路上傳遞絕不會被半路攔截或偷看

應用於檔案、圖資保護

- 把 3D CAD/BIM 圖資、與重要資料存在資料庫、備份檔或雲端空間時，系統會自動將資料亂碼化儲存
 - 即使資料庫遭存取或實體硬體遺失，沒有鑰匙的人拿到的只是一堆毫無意義的文字亂碼
- TLS 協定能確保檔案從雲端傳到使用者螢幕的過程中，建立一個加密的專用通道
 - 即使有惡意駭客在同一個公共 Wi-Fi 或網路節點竊聽，也只能看到加密過的傳輸封包，完全無法還原出原貌

資訊安全暨商業價值

評估項目	傳統事務所	您的事務所	帶給業主的商業價值
資安認證	僅有防毒軟體或個人硬碟	- ISO 27001/27017/27018 - SOC 2	省去數週的法務與資安審核
圖資防護	隨身碟、一般 Email 或非加密雲端	AES-256 靜態加密 + TLS v1.2 + 傳輸	金庫級安全，防止半路攔截
權限管理	密碼共用，所有人均可隨意下載	MFA 多因素驗證、最小權限原則與角色控管	杜絕內部人員越權下載或複製
災害備援	手動複製到外接硬碟，易受損	每日跨區 30 天備份	保障專案按時交付，工期不停擺

可以大聲的說：我們不只設計做得漂亮，資料防護更是符合國際設計規範！

要花多少錢？

雲端與服務訂閱 (持續性)

企業版 email	NT\$350~500 /人月
雲端備份	NT\$300~1,000 /月
密碼管理器	免費 ~ 250 /人月
AI 訂閱	NT\$600~1,000 /人月
MFA 多因素驗證	免費

硬體與實體設備 (一次性)

NAS 空機 (2~4 槽)	NT\$8,000~25,000
NAS 硬碟 (每顆 4TB)	NT\$8,000~12,000
外接備份硬碟 (4TB)	NT\$5,000~10,000
防毒 / 資安軟體	NT\$800~1,500 /年



小公司 (3~5 人)：設備一次性約 NT\$4~6 萬、每月訂閱制約 NT\$1,000~3,000

* 參考價格會因方案、容量、時間與匯率變動；不代表推薦特定產品，選型可個別討論

《30 日行動計畫》：一個月把基本防護建起來

WEEK 1

帳號與身分防護

- ✓ 重要 email / 雲端開 MFA 雙重驗證
- ✓ 盤點所有共用帳密，清理過期權限
- ✓ 全面改用獨立個人帳號登入系統

WEEK 2

落實備份機制

- ✓ 確認 NAS 外有第二份獨立備份
- ✓ 確保至少 1 份備份位於辦公室外 / 雲端
- ✓ 實際測試還原一個重要檔案

WEEK 3

權限與設備管理

- ✓ 製作到職 / 離職權限清單 / 檢查表
- ✓ 及時收回外包與離職人員存取權
- ✓ 確保電腦與設備開啟自動更新與密碼

WEEK 4

AI 規範與應變演練

- ✓ 訂定內部 AI 工具使用規範
- ✓ 擬定資安事件處置 SOP (隔離與通報)
- ✓ 定期執行資安演練與資安評估

六個問題自我檢核表

- | | | |
|---|---------------------------------|--------------------------|
| 1 | 資料 三年前的資料，5 分鐘內找得到 | ☐ |
| 2 | 存取 離職同事的帳號，已經完全連不進來 | ☐ |
| 3 | 備份 NAS 壞了，有備份檔案且親手還原過 | ☐ |
| 4 | 帳號 email 密碼被偷，對方也進不來（有設定 MFA） | ☐ |
| 5 | AI 哪些資料不能給 AI，清楚知道公司的準則與規範 | ☐ |
| 6 | 應變 資安事故發生，知道應變 SOP 步驟 | ☐ |

計分

0~2 分

從第一級開始

3~4 分

補齊第一級、往第二級

5~6 分

可規劃第三級與 AI 政策

04

第四部分 · AI 篇

讓 AI 讀你的資料

AI 工具的三種型態：依資料敏感度選型



免費版、個人版

- 資料傳至廠商雲端，可能用於 AI 模型訓練
- 適用情境
 - 對外文案、公開資料整理
- **注意事項**
 - 嚴禁上傳客戶個資、合約草稿、財務報表等

適合：公開資料、對外文案



企業 / 團隊版

- 簽訂商務條款，承諾資料部會拿去訓練模型
- 適用情境
 - 日常業務由建、會議記錄摘要、內部簡報
- **注意事項**
 - 仍須注意極度敏感之核心營業秘密與法規個資

適合：日常業務、內部文件



地端 / 自建版

- 100% 本地硬體計算，資料完全不出辦公室
- 適用情境
 - 未公開的圖面設計、合約條款、業主敏感資料
- **注意事項**
 - 需自行準備適當硬體與基礎維護能力

適合：競圖、合約、業主個資

常見的 AI 類型

模型	模型說明	適合情境	硬體門檻	小團隊建議
ML (Machine Learning)	傳統數據統計與預測模型	財務數據預測、客戶流失分析、Excel 表格分類	極低 (一般辦公電腦即可)	適合純數據分析，不需特別買 AI 主機
DL (Deep Learning)	專精於特定影像或語音辨識	scanned PDF 光學字元辨識 (OCR)、發票單據自動辨識	低 (標準電腦或基本顯示卡)	適合單一特定自動化任務
LLM (Large Language Model)	如 70B+ 參數以上的超大模型	複雜邏輯推理、跨領域深度分析、高難度文案撰寫	極高 (需數十萬至百萬級多顯示卡伺服器)	不建議地端自建成本過高；雲端旗艦模型表現更佳
SLM (Small Language Model)	如 1B~9B 參數輕量模型	內部公文/合約問答、SOP 查詢、RAG 知識庫	中 (單張 RTX 5060/5070 或 Mac Mini)	地端部署黃金首選！
VLM (Vision Language Model)	能同時看懂圖片與文字的模型	看懂設計圖紙、施工現場照片標註、PDF 附表解讀	中高 (需 16GB+ 之顯卡或 M 系列晶片)	有設計圖、現場照片、掃描檔需求者必備

地端 AI 的優勢是甚麼？



核心商業機密

商業機密未公開，研發構想、底價與產品圖面，絕對不能外流



個資與法規合規

合規與個資保護，含有個人資料與合約條款



內網隔離環境

不受雲端服務斷線與政策變更影響，確保核心業務100% 穩定運作



企業資產自主權

知識資產自主掌控，模型與 RAG 知識庫完全在地化

- 資料留在自有環境
 - 降低外洩風險，內部管控仍需須做好
- 自主控制權高
 - 可自行決定模型、系統配置、更新時機，較不受服務商政策或價格影響
- 離線可用性
 - 可設計無網路的環境下運作

為什麼企業需要 RAG？從「憑印象瞎編」到「開書考試」

RAG 能讓地端 AI 準確引述公司內部文件，RAG 就像給 AI 一本「企業專屬字典」，確保輸出精準、可查證



直接問它

通用 AI

- 運作方式：
 - 只靠模型預先訓練好的記憶回答
- 回答特徵：
 - 講得頭頭是道、語氣非常肯定，但可能引用舊版規範、別國法規，甚至自己胡編（產生幻覺）
- 致命痛點：
 - 無法追溯出處，答錯了找不到責任來源



先給資料再問

導入 RAG 的 AI

- 運作方式：
 - 先去知識庫搜尋最新檔案，再把內容交給 AI 整理回答
- 回答特徵：
 - 嚴格照著公司的 SOP、合規文件與合約回答，不憑印象
- 核心價值：
 - 精確附上出處（例如：引述自《2026 管理手冊》第 15 頁），有憑有據

情境問題

	製造與工程業	人資與內部行政
提問	這批零件的公差範圍是多少？	我剛滿一年，婚假有幾天？可以分開請嗎？
通用 AI	常見的機械零件公差通常為 $\pm 0.05\text{mm}$ ，如果不確定建議進行檢測。	根據勞基法規定，婚假為 8 天，原則上需在結婚登記日起 3 個月內請畢...
導入 RAG	依據《A3 型號產品品管規範》第 4 章，此零件公差上限為 $\pm 0.02\text{mm}$ 。若超出此範圍需走特採流程。（出處：QA_SOP_2025.pdf，第 18 頁）	公司提供 10 天給薪婚假（優於法規），可在半年內分多次申請，並需附上結婚證明。（出處：員工手冊_2026版_人事規章.pdf，第 8 頁）

讓地端模型讀你的資料

① 建立索引 (離線)



② 查詢問答 (線上)



檢索最相關片段

閉環：業界貢獻 → 知識庫越厚 → 地端 AI 回答越準 → 再回饋更多實務

部署地端 AI，需要準備什麼？



硬體設備

- 放置於辦公室內並連接內部網路即可運作，無需專用機房
- 入門首選
 - Mac mini (RAM 32G以上)
- 效能首選
 - 具備 NVIDIA 獨立顯示卡、RAM 32G以上



模型運算核心

- 負責載入開源大語言模型 (LLM) 並執行推論計算的後端引擎
- 推薦開源工具
 - Ollama、LM Studio、Jan



使用介面與知識庫整合

- 讓一般員工無需具備技術背景，透過瀏覽器即可像使用 GPT
- 推薦解決方案
 - Open WebUI (類似 ChatGPT 的操作介面)
 - AnythingLLM

評估指標	現有電腦就夠用	建議採購獨立主機 (10萬)
使用人數	1~2人偶爾查詢，文字順暢吐出，等待時間 < 3 秒	5人以上同時查詢，回答要等 > 15 秒
處理檔案類型	只讀純文字與PDF	需要 AI 看圖紙與照片，例如：解析 CAD、施工現場照片

地端 AI 並非萬能

地端 AI 的目的是『資料絕對掌控權與零外洩風險』，而不是一個世界最強大、最聰明的通用模型



能力上限：會比雲端笨一點

- 雲端模型：如 GPT-6、Claude Fable 5.1，擁有數千億甚至上兆參數與龐大算力集群支援
- 面對極度複雜的邏輯推理或邏輯創作，地端模型的回答品質遜色於雲端模型
 - 但若用於內部 SOP 檢索、公文回答與法規比對，地端模型配合知識庫已完全夠用



營運維護：需要指定內部管理員

- 模型迭代：開源模型技術更新極快，需定期手動升級至最新版本
- 知識庫更新與備份：當公司制度變更或新增專案資料時，需手動補充與重新索引

混合部署：兩全其美的策略

並非只能二選一，我全都要！



地端

- 高敏感客戶資料與個資
- 未公開圖資與競圖策略
- 商業合約與財務報表
- 內部 SOP 與法規檢索 (RAG)
- 工地敏感監造紀錄
- 核心產品設計



雲端

- 公開資料分析與趨勢整理
- 對外行銷文案與社群
- 無敏感資訊的腦力激盪
- 標案分析與提案簡報優化



今天回去做第一件事就好



把 email 的多因素驗證 (MFA) 打開



工作能力



現金



信譽



設計資產

資安常見問題 Q&A

「我們才 3 個人，有必要嗎？」

資料顯示高達 96% 的勒索軟體受害者都是中小型組織

「平時是用 Google Drive 或 OneDrive 同步資料，這樣算是有備份嗎？」

同步不等於備份，同步的目的是「讓兩邊資料保持一致」

「MFA 很麻煩，每次要用手機。」

非常有必要！開啟 MFA 就能擋掉超過 99% 的帳號盜用風險

「我們又沒有機房，也沒有獨立申請 ISO 認證，要怎麼向業主證明資安合規？」

選用已通過 ISO 27001、ISO 27017/27018 與 SOC 2 Type 2 國際認證的雲端服務與軟體

「外接備份硬碟一直插在 NAS 或電腦上自動備份，這樣安全嗎？」

非常危險！備份完成後應將硬碟實體拔除，離線的硬碟是任何軟體都無法攻擊到的

「資安防護做得再好，遇到突發硬體故障或勒索病毒時，第一步該做什麼？」

應具備明確的「資安事件處置 SOP」

AI 常見問題 Q&A

「員工私下使用免費版 ChatGPT 幫忙寫公文或處理圖資，會有什麼風險？」

免費版或個人版 AI 工具會將使用者上傳的對話與文件傳至廠商雲端，並可能用於 AI 模型的二次訓練

「公司應該完全禁止同仁使用 AI 工具嗎？」

禁不了也不該禁，要做的是「訂定明確的 AI 工具使用規範」

「直接開啟 NAS 內建的 AI 搜尋功能方便嗎？有什麼陷阱？」

若NAS 內部的資料夾沒有做權限隔離，基礎資安沒做好，開啟 NAS 內建 AI 等於把 AI 變成內鬼！

「我們事務所的歷年專案資料非常混亂，是不是就無法建立 AI 知識庫了？」

不需要全部整理好才能開始，可選定一個主題陸續建立

「AI 未來會不會完全取代建築師或專業設計師」

AI 取代不了專業簽章、法律責任與空間設計判斷

「建立好地端 AI 知識庫後，會不會反而讓公司機密更容易被員工外流」

知識庫必須綁定「角色的權限控管」，搜尋與回答僅限該員工原本有權讀取的資料夾內

歡迎加入 EagleAI 群組！



Reference

參考資料