

# 資安治理

## 建立具備高度韌性的智慧醫療環境

衛生福利部資訊處 李建璋

NotebookLM

# 觀念轉型：資安就是病安

| | 過去 | 深耕計畫新思維 |
| --- | --- | --- |
| 核心責任 | 資訊部門的技術問題 | 攸關病人安全與醫療持續性的全院命脈 |
| 防禦假設 | 完美阻擋邊界外的駭客 | 假設必然遭入侵 (Assume Breach)，<br>著重「韌性」 |
| 投資定位 | 滿足法規的最低門檻 | 爭取深耕計畫加分的主動性投資 |

智慧醫療科技以資料為核心，若無安全可信賴的環境，
不僅個資外洩，更將導致醫療系統全面停擺。

NotebookLM

# 現代醫療面臨的系統性威脅

## 攻擊型態

已經高度產業化、組織化，
進入 AI Agent 自動化攻擊時代。

## 地緣政治

臺灣醫院已成為全球駭客高
頻率攻擊的重點目標。



## 入侵管道

90% 以上透過供應鏈漏洞、VPN
弱點、釣魚郵件與社交工程入侵。

## 致命戰術 (雙重勒索)

駭客透過橫向移動與權限提升，不
僅加密病歷，更竊取資料威脅公開，
甚至刪除雲端備份以摧毀復原能力。

NotebookLM

# 勒索軟體三階段應變指引

## 第一階段：立即控制災害 (Control)

第一時間斷開受感染網路，控制傷害範圍，快速辨識病毒特徵與感染來源。

## 第二階段：系統復原 (Recover)

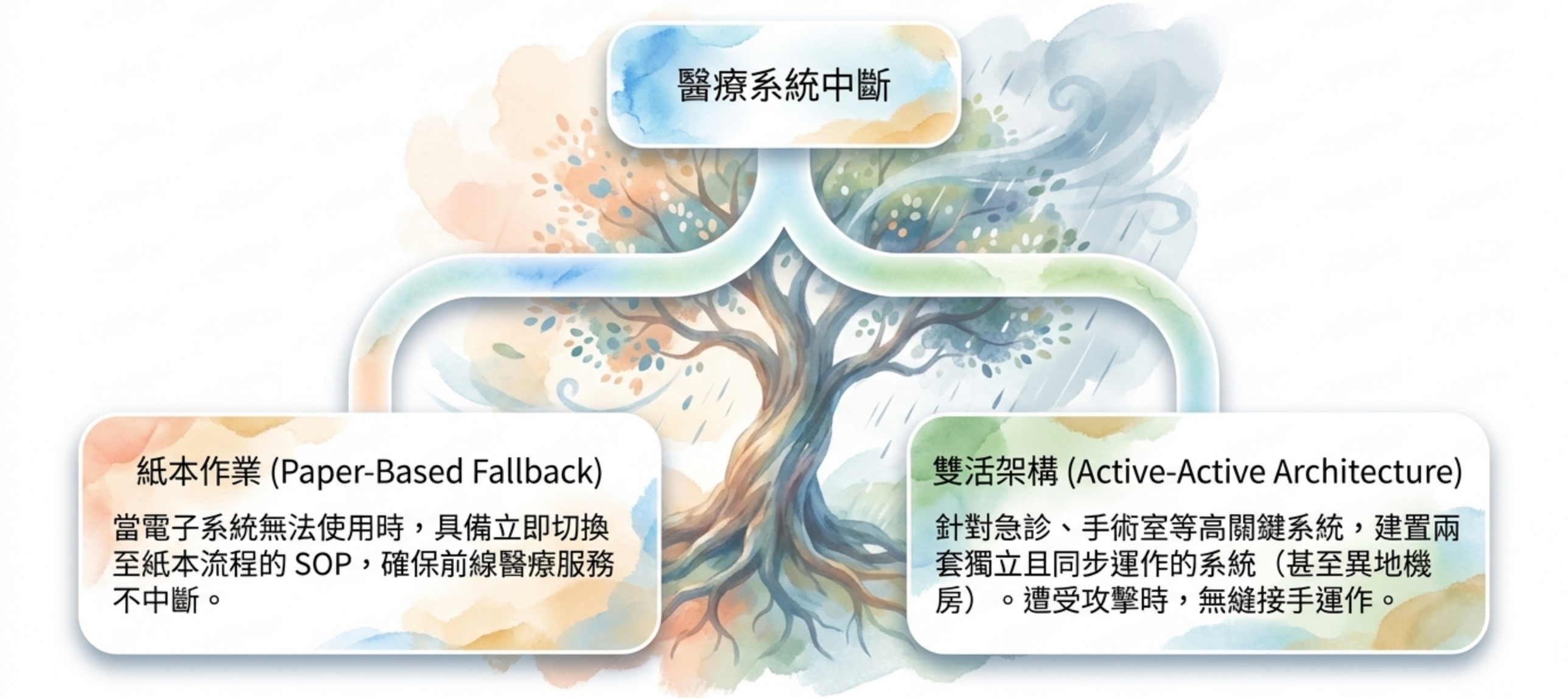
確認惡意程式完全清除後，利用乾淨的備份資料逐步恢復醫療資訊系統，確保服務持續。

## 第三階段：調查與重建 (Investigate & Rebuild)

完整的事件通報、證據保存、事故調查，以及事後檢討與系統重建。

NotebookLM

# 落實營運持續：超越紙本的真實備援




NotebookLM

# 運用 AI 主動防禦零時差攻擊 (Zero-day Attack)




### 自動掃描 (Scan)

利用 AI 工具 (如 Claude mythos，微軟 mDASH 多代理人平台，ChatGPT 5.5) 自動分析系統狀態與原始碼。

### 辨識弱點 (Identify)

快速找出潛在漏洞與安全盲點。

### 修補建議 (Patch)

AI 自動提出修補建議，建立持續性的自動化安全檢測流程。

深耕計畫鼓勵利用經費，優先針對重要核心系統導入 AI 輔助掃描，提早防堵零時差風險。

NotebookLM

# 內部防線：最小權限原則與行為監控

## 傳統高階主管權限

因職位高而自然擁有全系統存取權
(風險：非業務相關查詢、濫用個資外洩)。

## 最小權限原則

每位使用者僅能取得完成工作必需的最低權限。合理限縮跨部門與高階管理者權限。



導入使用者行為分析 (UBA)，主動持續監測異常存取、異常查詢或其他可疑行為。

NotebookLM

# 從攻防測試到全院「韌性演練」




唯有透過全國性實戰演練，才能在真正遭遇勒索軟體時，第一時間做出正確判斷。

NotebookLM

# 生成式 AI 部署的資安治理矩陣

## 主權雲端服務 (Sovereign Cloud)

核心規範：資料必須儲存於臺灣境內資料中心。

安全機制：傳輸及儲存全程加密。業者資料庫管理者不得直接存取內容。

禁止事項：不得將使用者資料用於模型再訓練 (未授權用途)。

## 地端部署 (On-premises LLM)

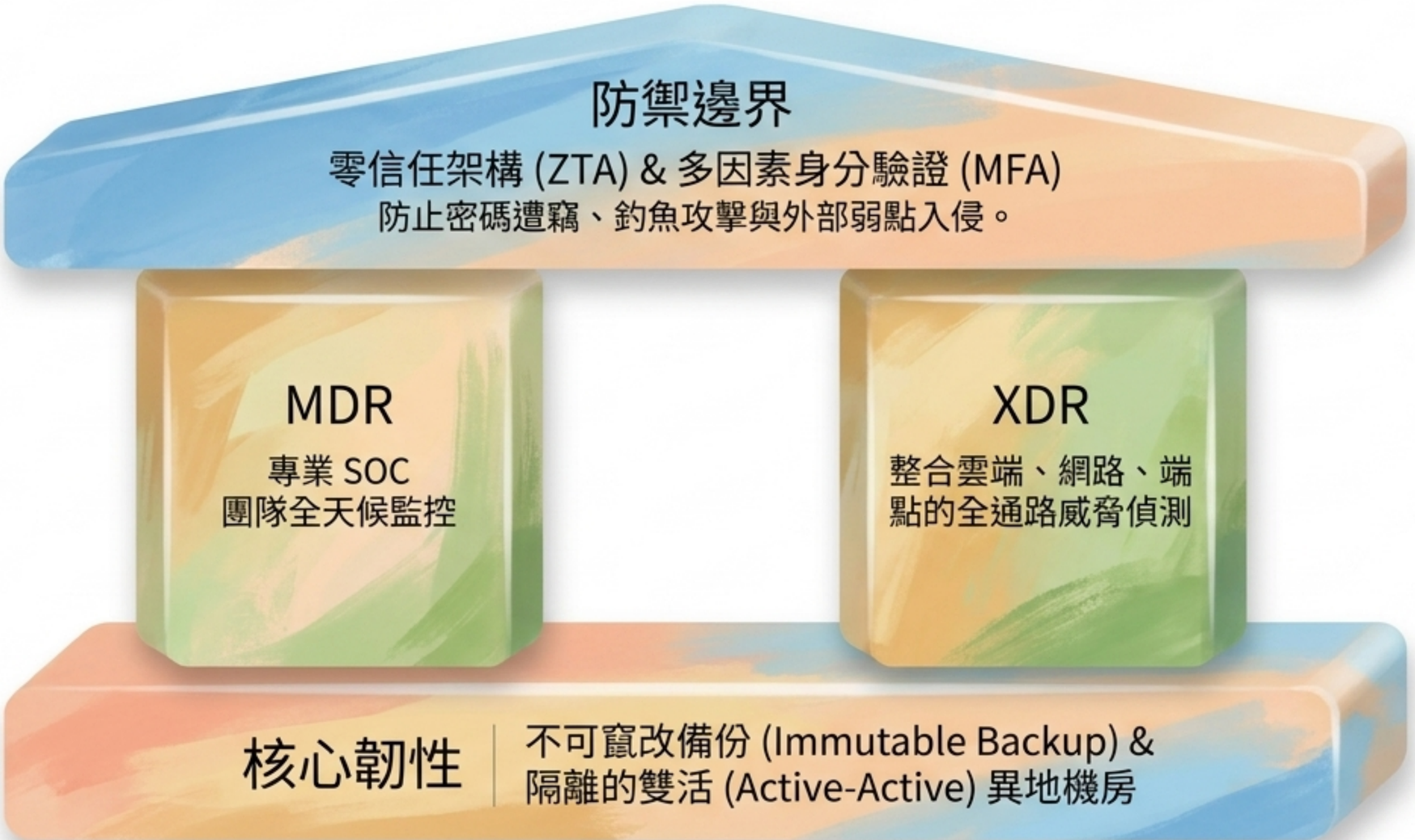
核心風險：大量使用紀錄 (Log) 若遭竊，仍可還原病患個資。

安全機制：建立完整的 Log 存取控制、加密保存與定期清除機制。

準確度維護：建立人工審核 (Human-in-the-loop)，持續進行 RAG 資料庫維護與模型微調。

NotebookLM

# 深耕計畫鼓勵投資的新興資安藍圖



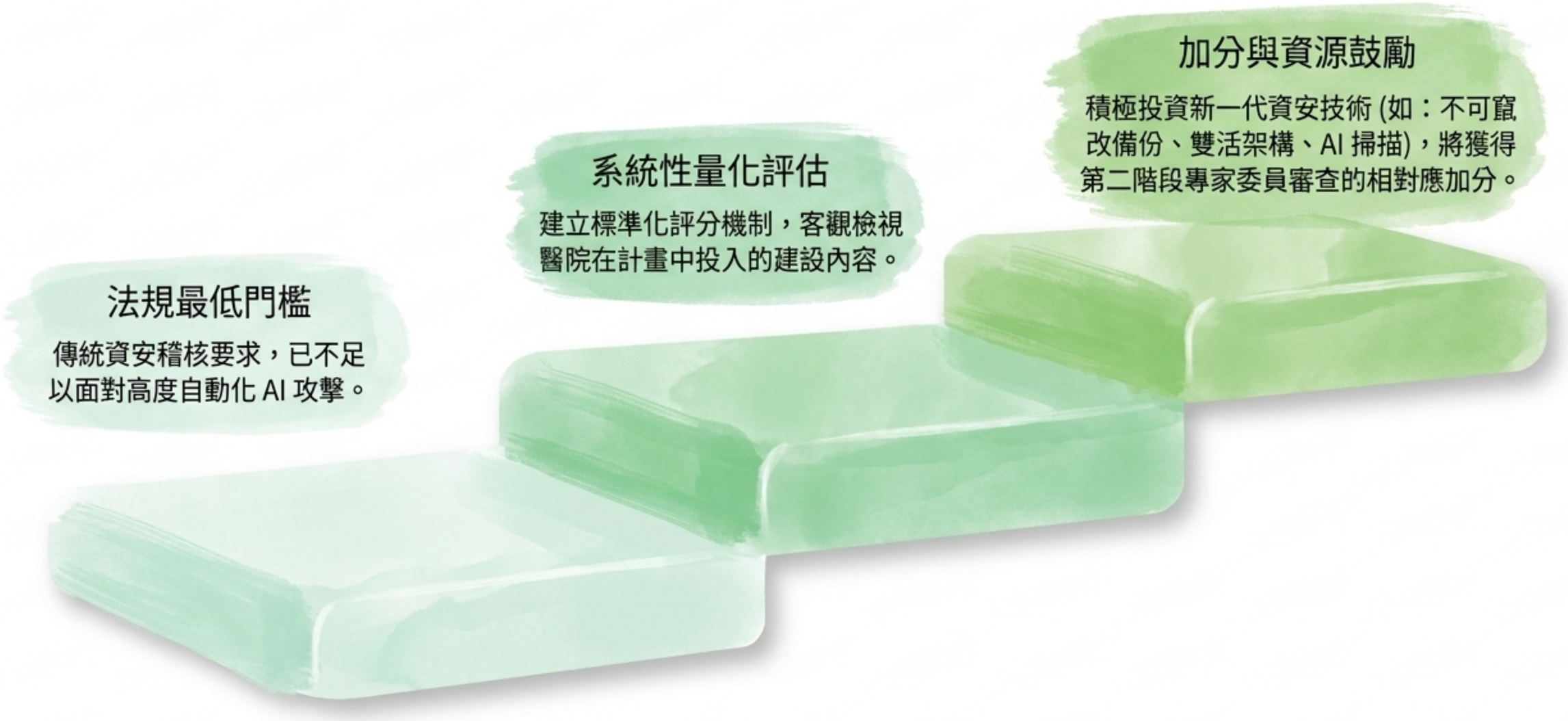

NotebookLM

# 實戰防護：破解雙重勒索 (Double Extortion)




NotebookLM

# 深耕計畫：量化評估與資源引導




NotebookLM

# 投資下一代資安，就是投資病患的未來

隨著駭客攻擊技術快速演進，唯有將資安視為醫療基礎建設的最核心，積極投入具備高度韌性的智慧醫療環境，才能真正實踐「資安就是病安」的終極承諾。



NotebookLM