



# AI 組合戰略 × 韌性自檢卡

AI Portfolio × Resilience Self-Audit

S3-1 COMPANION · stratpilot.substack.com

如果你的全部 AI 工作流綁在一個供應商上，今天就是修復日。

Single-vendor AI stack = single point of failure.

## A 生態位地圖 Ecosystem Map

**FLASH** 高頻、低複雜度：摘要、分類、模板填空。便宜模型就夠，不必動用旗艦。

**SONNET** 日常寫作、結構化分析、中等推理。這是你 70% 任務的真正落點。

**OPUS** 高風險判斷、多層推理、長篇拆解。只在需要穿透時啟用，避免習慣性依賴。

## B 三層解耦 Three-Layer Decoupling

01

身分層  
Identity

帳號、訂閱、付款方式。供應商變動時，這一層最貴、最難搬。

02

資產層  
Assets

Prompt、knowledge base、chat 歷史。用本地或獨立雲端存，別鎖死在平台。

03

算力層  
Compute

實際執行的模型。保持 2 家以上可快速切換，推理管線抽象化。

## C 自檢題 Self-Audit Questions

- ☐ 01 我的 AI 訂閱是否集中在 1 家供應商？如果是，我承擔的風險是什麼？
- ☐ 02 我的 prompt 與 knowledge base 存在哪裡？能否在 1 小時內匯出？
- ☐ 03 供應商 down 24 小時，我手上有沒有能接住關鍵工作的 B 計畫？
- ☐ 04 我的任務是否都在用旗艦模型？有沒有該降階卻沒降階的？
- ☐ 05 過去 30 天，我換過模型或平台嗎？還是習慣性停在同一個？

### 🎯 坐標錯配診斷 · Coordinate Misalignment

你以為在做「AI 工具選擇」，其實在做「供應商綁定」。真正的決策不在模型能力表，而在你把哪一層交出去。

本卡為自檢工具，非投資建議；供應商風險請以官方公告為準。

作者 StratPilot

系列 組合戰略

版本 v2 · 2026-04

StratPilot

《對齊與理解》





# Claude 模型路由卡

Claude Model Routing Card

任務 → 階層 → 機型 Task to Tier to Model

stratpilot.substack.com · v1 · 2026-04

## 路由表 Routing Table

| 任務類型 · TASK      | 階層 · TIER | CLAUDE | 成本 · COST |
|------------------|-----------|--------|-----------|
| 摘要，重述，翻譯         | 低 LOW     | Haiku  | 1×        |
| 模板填空，分類，標籤       | 低 LOW     | Haiku  | 1×        |
| 結構化分析（含幾步推理）     | 中 MID     | Sonnet | 5–7×      |
| 中等寫作（blog，報告）    | 中 MID     | Sonnet | 5–7×      |
| 創意發想（無對錯）        | 中 MID     | Sonnet | 5–7×      |
| 不可逆判斷（簽約，發布，刪資料） | 高 HIGH    | Opus   | 25–30×    |
| 多層推理，長篇拆解        | 高 HIGH    | Opus   | 25–30×    |
| 高風險領域（法規，醫療）     | 高 HIGH    | Opus   | 25–30×    |

默認 Sonnet。Haiku 是省錢路徑，Opus 是保險路徑。

決定權在「任務性質 + 不可逆程度」，不在「習慣哪個」。

作者 StratPilot

系列 組合戰略

版本 v2 · 2026-04

StratPilot  
《對齊與理解》





# 三層解耦 Migration Checklist

## Three-Layer Decoupling Migration Checklist

AI 工作流韌性自檢 → Resilience Self-Check for AI Workflows

stratpilot.substack.com · v1 · 2026-04

### L1 身分層 Identity Layer

- ☐ I-1 主帳號用固定 VPN 或網路地址（避免被風控誤判為共用）。
- ☐ I-2 2FA 備份加上支付多元化（避免帳號永久失效）。

### L2 資產層 Asset Layer

- ☐ A-1 System prompt 或 Persona 文件版本控管（git 或 Obsidian）。
- ☐ A-2 Skills 或 Projects 用標準格式（markdown 加 YAML）保存，避免綁死單一供應商。
- ☐ A-3 對話沉澱結構化（決策記錄，知識卡），不依賴某家 memory feature。

### L3 算力層 Compute Layer

- ☐ C-1 至少 2 家供應商並行訂閱：單家中斷或漲價不致全工作流停擺。
- ☐ C-2 路由策略文件化（呼應 Claude 模型路由卡）。

### T 觸發節點 Triggers

- ☐ T-1 帳號被風控或 IP 異常警告。
- ☐ T-2 訂閱漲價超過 30% 或服務條款重大變更。
- ☐ T-3 行業重大政治或合規事件（單一供應商風險上升）。

**三層獨立 = 任一層斷裂不致全停。**

檢查不是儀式，是 30 分鐘可觸發 fallback 的能力。

