專題演講　#Agentic AI　#Multi-Agent治理

讓 Agent 安全上工：金融產業多雲環境 Multi-Agent 的治理與國際標準合規實踐

Google Cloud 台灣技術總經理｜林書平 Harry Lin

13:30–13:50　有效內容 **26.1** 分鐘　逐字稿 **11,110** 字

核心框架

這場不談產品細節，而是給出一套**Agentic Enterprise Framework**——企業要開發、管理、治理 Agent 時，由下而上該看哪些層：

```
Agent Service（最上層）
Agent Management / Operation
Security
Data
Infra
```

Agent 時代的三大支柱

1. **Tokenomics（Token 經濟學）**——Agent 不再只做單一件事，而是整合一整條流程，Token 消耗自然大增。關鍵問題是：**流程的每一個 phase 都一定要用最貴的 Frontier Model 嗎？**
2. **Business Process 與 Value 的整合**——必須整合進業務流程與價值，才看得到 Agent 的價值
3. **Security**——任何新技術採用時永遠最重要

一、Infra 層：Inferencing 不是 Training

Harry 用武俠小說比喻兩者的差別：

	Training	Inferencing
比喻	**練功**	**戰場上即時回應**
特性	大量吸取資訊、成千上萬 GPU/TPU 串連、運算數百億參數	需要低 latency 與充足 context

Agent 大部分工作是 inferencing，且互動模式是**來來回回的**——你問、它答、你補 context、它給更多資訊。這意味著 Agent 要即時且正確回應，靠的是 **Context**（也就是 Agent Session／Agent Memory）。

硬體的具體回應：Google 自研 TPU 第八代把 Training 與 Inferencing 分開，**Inferencing 的 Memory 是第六代的 3 倍**；NVIDIA GPU 也為 agent inferencing 做了對應調整。

二、Data 層：AI Ready Data

問題的根源

企業既有資料**不是 design for agent，而是 design for human**——Database schema 是從人的角度、按 business process 設計，再由人寫程式下 query。

三個因此產生的落差：

1. **Scalability**——Google CEO Sundar 的 vision 是內部未來至少有**幾萬個 agent** 執行所有 operation。當 agent 數量以萬計、處理速度極快時，後端 database 與 storage 撐不撐得住？
2. **Context**——過往很多 context 存在人的大腦裡。做供應鏈的人知道整條供應鏈的業務脈絡，但 agent 看到資料時沒有這個脈絡
3. **Security Control**——過往是給人或程式一個 authority。但**同一個 agent 會被經理、處長、副總同時使用**，這個 authority 該怎麼做資料控管？

Context 的三個層次

層次	內容	例子
Technical Metadata	Schema、欄位、型別與意義	這個欄位是 Integer，代表信用卡消費金額
Business Semantics	這些技術欄位背後的業務意涵	這個 Campaign 打的是什麼族群、什麼地區
Personalization	不同角色與同一 agent 互動時要的資料不同	副總看全台灣，區域經理只看自己區域的消費族群特性

Multi-modality 帶來的新資料來源

Agent 不只看得懂文字——影片、聲音、圖片都能解析出意義。以行銷活動為例，除了活動數量、參與人數等文字資料，**Campaign 的影片與宣傳圖本身也是 Context**，agent 可以把它們轉化成 Business Context。

三、Security 層：用魔法打敗魔法

> 「現在的 Hacker 也用 AI 來 create 他的 Attack Campaign……**這相當於人家在用魔法，我不可能拿著木棍木槍去跟槍砲打戰。**」

攻擊面的變化：AI 生成的釣魚 email 與連結、**多模態讓對方甚至能打一通 deepfake 語音電話**給你做驗證。

為什麼 Security 特別適合用 Agent

三個特性：資料量非常龐大、有一定 pattern、流程可以自動化。

實際成效：第一層 Alarm Triage 至少可達 98% 的 reduction。

Security 人員的兩種痛苦： - **False Positive（誤判）**——不是攻擊卻被判成攻擊，要花大量時間確認 - **False Negative（漏判）**——更可怕，「只要漏判一個，你就被 Penetrate 進去」

Triage 之後的完整自動化鏈：收集對應 Log 與資料 → Analyze → 對應到 CVE 編號 → 決定該 Tag 什麼 Action → Post Action。

另一個角度是 Development 階段的安全：應用服務部署上線後，從 Container Runtime、Application、Agent 到 Model 各層都可能有 Vulnerability，可用 Agent 掃描整個環境。

四、Agent Management 層：生態系與新的攻擊面

Agent 生態系的主要元件：**Agent 本身、Model（大腦）、Tool（MCP、Skill）、API（整合 SaaS）**；元件之間透過 A2A 或 HTTP/RESTful API 溝通。

這些溝通衍生出兩個治理議題：

Agent Supply Chain

概念與 Software Supply Chain 完全相同——過去攻擊者 hack 你用的 Library，就能從中擷取你 Application 的資產。**現在 Agent 就像 Application，你呼叫的 API、你用的 MCP、甚至你 Skill 裡的 Context 都可能被 Poison。**

Data Access Control

Memory / Context Poisoning——如何透過這種方式引導你的 Agent 或 LLM 洩漏不該揭露的資料。

> **OWASP 已推出 Agentic Application 的 Top 10**（過去是 Application Layer 與 Data 的 Top 10 攻擊），這是金融業合規可直接對照的國際標準。

五、Enterprise Agent Platform 的四個治理角度

階段	要處理的事
Build	不同 Model、Agent Framework、Agent Development Kit（如 ADK 與各種 Open Source）
Scale	成千上萬個 Agent 的 Runtime；**Long-term Context 與 Short-term Session 的管理**——讓 Agent 記得你幾個月幾年來的習性，同時區分這個 session 在談 Travel、那個在談 Development
Governance	**Agent Registry**（每個 Agent 有 ID，ID associate 到被賦予的 authority 與可存取資料）、Identity、Policy、Agent Gateway 的 Input/Output 控管
Optimize	持續監控 Agent 的使用與 Response Quality，據以分析流程該拆成哪些 phase、每個 phase 該呼叫哪個模型

Context Engineering 的必要性

Agent 互動累積的 Context 會越來越長，導致執行效率問題，且**幾年前的 Context 可能被擠掉**。因此需要在 Session/Memory 中 Summarize——「**有點像是精華記憶萃取，你不會保留一些無關緊要的東西。**」

Optimize 與 Tokenomics 的連結

最簡單的方式當然是把所有 task 都交給最先進的 Frontier Model——「這一定是可行的方式，**但從 Cost 的角度這是你願意做的方式嗎？**」唯有監控 Agent 的產出品質與 Log，才有辦法判斷哪些 phase 可以用 Flash 這類

CP 值高的模型，哪些真的需要高階 Reasoning。

可行動要點

- **OWASP Agentic Application Top 10** 可直接作為金融業 Agent 平台的資安檢核基準
- AI Ready Data 的三層 Context 模型（Technical / Business / Personalization）可用來盤點現有資料缺口
- Agent Registry + ID + Authority 的設計，與場次 03、05 提到的「數位同事獨立身份」是同一件事的不同說法
- Security Agent 的 98% alarm reduction 是可對標的量化預期

2026 國泰金控技術年會．會後整理的閱讀筆記，非官方發布內容。錄影以 openai-whisper large-v3 轉寫後校閱，講者姓名與職稱已對照官方議程核正。人名、數字與專有名詞建議對照影片核實。