力旺電子 2026 Q1 線上法說會講稿

2026 年 5 月 8 日, 16:00-17:00

開場致詞

徐清祥, 董事長

各位股東和投資先進，今年第一季，力旺電子營運表現持續創下歷史新高。除了 3 奈米授權在 AI Server CPU 應用持續成長之外，我們也成功拓展至高速傳輸介面等新領域。

同時，隨著 AI 基礎架構快速演進，產業對硬體安全的需求正全面升級。Open Compute Project（OCP）於 2025 年提出的 Foundation Chiplet System Architecture（FCSA），明確要求 Chiplet 系統中的每一顆晶片都必須具備 Hardware Root of Trust。這代表未來 AI 系統中的每一個 Chip，都將需要內建硬體安全機制，以確保系統可信度與資料安全。

此外，Agentic AI 的快速發展，以及各國政府對後量子密碼（Post-Quantum Cryptography, PQC）安全要求的提升，也正推動全球迎來過去二十年來最大規模的硬體安全升級浪潮。因應這樣的趨勢，我們正積極由 IP 供應商進一步邁向系統級安全解決方案供應商。我們自主研發的 Hardware Security Module（HSM）產品，也將在通過美國 NIST 驗證後，正式授權終端客戶導入量產。我們相信，力旺將會是這波全球硬體安全升級趨勢的重要受惠者。

另一方面，力旺最核心的技術基礎仍然是 Logic NVM。我們長期專注於利用標準邏輯製程（Logic Process）實現非揮發性記憶體技術，相關技術除了可以以 IP 形式嵌入 SoC，也能進一步發展為 Standalone 記憶體產品。

近期全球 Flash 記憶體供應持續吃緊，而力旺的技術優勢，在於能夠直接活化成熟邏輯製程產能來生產非揮發性記憶體，因此不受限於傳統 Flash 專用產線的產能瓶頸。目前我們正積極與多家晶圓代工廠合作推動相關技術與產品化進程。這不僅對代工廠與終端系統客戶具有高度策略價值，也可望繼 OTP 與 PUF Security 之後，成為力旺下一階段重要的營收與獲利成長動能。

接下來，我們請財務主管夏喬威先生說明 2026 年第一季營運報告。

營運報告

夏喬威，財務主管

第一季營運結果

各位股東，午安。

首先，我就先針對 2026 年第一季的營運結果向各位作個報告。

在營收方面，本季營收為新台幣 1 拾億 9 仟 3 佰 9 拾 9 萬 3 仟元，較前一季成長 4.4%，比去年同期成長 20%。

在營業費用方面，本季營業費用為 4 億 3 仟 1 佰 6 拾 1 萬 6 仟元，較上一季增加 4.6%，比去年同期增加 10.8%。

在營業淨利方面，本季營業淨利為 6 億 6 仟 2 佰 3 拾 7 萬 7 仟元，較上一季成長 4.2%，比去年同期成長 26.8%。營業淨利率方面，較上季下降 0.1 個百分點為 60.5%，比去年同期上升 3.2 個百分點。本季淨利為 5 億 9 仟 6 佰 2 拾 5 萬元，較上一季成長 5.9%，比去年同期成長 29.1%。

總結，2026 年第一季的 EPS 為新台幣 7.98 元。

在總體營收中，我們分授權金及權利金來做說明：

1. 首先，第一季的授權金佔本季營收 34.8%，金額較上一季增加 9.9%，比去年同期增加 58.6%。以美元計算，季增 7.8%，年增 64.4%。
2. 在權利金方面，權利金佔營收比重為 65.2%，金額較上一季增加 1.6%，比去年同期增加 6.2%。以美元計算，季減 1.2%，年增 11%。
3. 2026 第一季的總營收比上一季成長 4.4%，與去年同期比較成長 20%。以美元計算，季增 1.8%，年增 25.2%。

第一季營收貢獻分析

在整體營收中，再以各個技術對營收貢獻來區分：

1. **NeoBit** 貢獻了本季 20% 的總營收。本季授權金較上一季衰退 28.4%，比去年同期衰退 13.7%。在權利金部分，NeoBit 較上一季成長 3.1%，比去年同期衰退 4.2%。
2. **NeoFuse** 對本季的營收貢獻為 59.8%，本季授權金較上一季成長 39.8%，比去年同期成長 20.7%。在權利金部分，NeoFuse 較上一季成長 0.5%，比去年同期成長 7.4%。
3. **以 PUF 為基礎的 Security IP** 在本季貢獻 12.2%的營收。本季授權金比上季成長 21.5%，比去年同期成長 606.9%。權利金大幅成長至占權利金貢獻 1%。
4. **在 MTP 技術方面**佔總營收 8%。授權金比上一季衰退 5.5%，比去年同期成長 37.9%。權利金貢獻較上一季衰退 3.1%，較去年同期成長 45%。

第一季營收分析–Wafer Size

若以 8 吋及 12 吋晶圓區分：

1. **8 吋晶圓**權利金，佔第一季權利金營收的 33.7%，較上一季減少 5.5%，比去年同期減少 15.9%。以美元計算，季減 8.2%，年減 12%。
2. **12 吋晶圓**權利金，佔第一季權利金營收的 66.3%，較上一季成長 5.6%，比去年同期成長 22.5%。以美元計算，季增 2.8%，年增 28%。

第一季完成的已授權設計定案有 139 個。在 management report 中會詳細說明。

接下來，我們請總經理何明洲先生對未來展望做說明。

未來展望

何明洲，總經理

大家好，接下來我會向各位報告未來展望。

授權金方面：由晶圓代工廠與晶片客戶的授權數量增加以及平均授權單價提升所驅動。對於先進製程、 AI 相關應用、安全相關需求及新型 flash 授權需求非常強勁。

權利金方面：權利金加速成長，成長動能來自於既有產品 upgrade、新增先進製程應用單價提升、PUF 權利金收入擴大及具較高權利金費率的 MTP 產品占比上升。

新 IP 技術進展

1. 2nm 以下 OTP 及 PUF based security。
2. Neoflash 拓展至 1T Flash embedded 及 standalone flash。

商務平台擴展

1. Chiplet Security 平台
   我們正與生態系夥伴合作，開發端到端（End-to-End）的 Chiplet 安全解決方案，涵蓋供應鏈安全（Supply Chain Security）、Chiplet 身份驗證（Authentication）、安全通訊，以及 Hardware Root of Trust 等關鍵技術，以因應 AI 與異質整合架構下日益重要的晶片安全需求。
2. Data Center Caliptra 平台
   針對資料中心與 AI Server 市場，我們開發以 PUFrt（PUF-based Root of Trust）結合 Security Subsystem 的完整 IP 平台，協助客戶快速導入符合 Caliptra 架構與未來資料中心安全標準的硬體安全解決方案，加速客戶在新世代 AI 基礎建設中的 adoption 與產品量產。
3. Root of Trust / CPU 平台合作
   我們的硬體安全技術已成功整合至主要 CPU 供應商最新世代的 AI/AGI CPU 平台中，提供晶片層級的 Root of Trust、安全啟動（Secure Boot）、裝置身份識別與安全金鑰保護等功能，強化 AI 系統從晶片到系統端的可信度與安全性。
4. HSM Edge Server 平台
   我們以 PUF 為核心所開發的 HSM Edge Server，定位為未來「Security as a Service（SECaaS）」平台的重要基礎架構。此平台可支援汽車、醫療、工業控制、Edge AI 與高安全需求系統中的 Secure OTA、隱私保護、裝置身份管理，以及後量子密碼學（PQC）遷移等關鍵應用，協助客戶建立可持續升級的新世代安全架構。

接下來，我把時間交給數位行銷主管徐浩先生。

專題演講

徐浩，數位行銷主管

(Page 13: Hardware Security for AI Agents)

各位午安，感謝各位蒞臨。

過去幾年，AI 產業投入大量資源打造能夠「行動」的代理（agents），但卻沒有投入足夠時間建立讓這些行動「值得信任」的基礎。

而這個關鍵的安全需求，正是我們今天要討論的核心。

(Page 14: When AI Agents Reach the Real World, Security Must Be Absolute)

AI agent 並不是聊天機器人。聊天機器人負責「回答」，而 agent 則負責「行動」。它在一個循環中運作：蒐集情境 → 進行推理 → 做出決策 → 在現實世界執行 → 記錄結果 → 再重複。

這個循環有三個重要特性：

第一，它是自主的（autonomous）。Agent 會自行決策，中間沒有人工逐步核准。

第二，它以機器速度運行。每分鐘可能做出上千次決策，沒有任何合規人員或安全團隊能即時介入——這在數學上是不可能的。

第三，也是關鍵的一點，不同步驟的風險差異極大。在內部推理階段，錯誤仍可修正；但一旦涉及外部世界——資金、合約、身份或基礎設施——風險即變成不可逆。資金轉帳無法撤回，合約簽署無法召回。

(Page 15: Integrity Risks are Mostly Solved, Authorization Ones are Not)

在 agent 的每一個步驟中，都存在兩類風險：

第一是**完整性風險（Integrity Risk）**，也就是 agent 是否基於正確資訊運作：是否被餵入錯誤資料、推理模型是否被替換、記憶是否遭竄改。

第二是**授權風險（Authorization Risk）**，也就是 agent 是否「被允許」執行該行為：該行動是否經人類授權、agent 的身份是否真實。

這兩者是本質上不同的問題。然而市場目前的盲點在於：多數安全機制只處理「完整性」（例如軟體簽章、模型驗證），而「授權」則仰賴軟體政策，而這些政策是可以被繞過的。

如果兩者沒有同時解決，就無法真正治理：

- 正確模型執行錯誤授權 → 仍是災難
- 被授權的 agent 使用被竄改的邏輯 → 仍是災難

兩個面向都必須同時安全。而現今的 AI 系統，並未做到。

(Page 16: Real Governance Can’t Be Achieved Without Hardware Root)

目前所有主要的 AI 監管框架——包括歐盟 AI 法案、美國治理機制、金融監管準則——都逐漸收斂到四項要求：

- 高風險決策需有人類介入（Human-in-the-loop）
- 防竄改稽核紀錄（audit log）
- 模型保護
- 零信任身份驗證（zero-trust authentication）

所有 AI 廠商都宣稱能提供這些能力，但現行做法有一個致命問題：全部建立在「軟體」之上。

在缺乏 PUF（Physical Unclonable Function）的情況下，單純依靠軟體並不足以提供真正安全性，尤其如右側所示：

- 軟體簽章（software signatures）可被偽造
- 軟體稽核紀錄（software audit trails）可被具備足夠權限的人改寫
- 軟體金鑰（software keys）可能遭到提取
- 軟體身份（software identity）可被冒用

結果就是——現今的 AI 治理，本質上只是「治理的表象（governance theater）」：看起來合規，但無法抵禦真正的攻擊。要讓治理「可被強制執行」，而非「理想承諾」，唯一方法是將其建立在無法複製、無法提取、無法修改的基礎上——也就是硬體。

更精確地說，必須是晶片本身的特性：每顆晶片皆具唯一性、在需要時即時生成，且從未被儲存在任何可能遭竊取的位置。而這一切的核心，正是 PUF。

(Page 17: The Hardware-Anchored Trust for Agentic AI)

我們提供的是基礎層——硬體信任根（Hardware Root of Trust）。在這個基礎上，可以實現三個軟體無法提供的核心能力：

1. **身分（Identity）**。每一個 AI agent、設備、晶片或端點，都擁有不可偽造的硬體身份。這個身份來自物理隨機性，無法被複製——甚至連晶圓廠都無法重現。
2. **完整性（Integrity）**。模型、提示（prompt）與 agent 邏輯會被鎖定於授權硬體上。即使模型檔案被竊取，也只是無法解密的資料。因為不存在可被一併竊取的金鑰檔案——金鑰從未被寫入或儲存。
3. **權限（Authority）**。人類審批、稽核紀錄與政策執行，不再只是流程承諾，而是具備密碼學強制力。稽核紀錄不再只是「系統說發生了什麼」，而是可以被第三方驗證、甚至在法律上成立的證據。

AI 治理平台、agent orchestration 工具，以及合規監控儀表板，確實都具備重要價值，也正在建立實際商業模式。而 eMemory 的定位，正是在這些系統所共同依賴的底層硬體基礎。

總結而言，透過將安全機制從軟體層下沉至矽（silicon）本身，eMemory 能夠讓 agentic AI 在金融、醫療以及自主化基礎設施等高風險產業中，以真正具備自主性與權限控管的方式運作。

以上就是我們本次的分享內容，謝謝您的聆聽。

接下來，我們將進入 Q&A 環節。

結論

徐清祥，董事長

如果大家想了解更多有關公司在安全 IP 的進展，歡迎上 PUFsecurity 的官網 https://www.pufsecurity.com/上看，有很多文章跟課程。

我們會不斷努力的創新，提供客戶更好的 IP 與安全解決方案，也會為股東帶來更高的回報。公司會持續朝向每顆晶片都會用到我們的 IP 的目標前進。感謝各位股東長期對力旺的支持!