力旺電子 2026 Q2 線上法說會講稿

2026 年 8 月 14 日, 16:00-17:00

開場致詞

徐清祥, 董事長

各位股東、各位投資先進，大家午安。

首先，我想跟各位報告公司在 Security IP 方面的最新進展。

過去幾年，我們的 Security IP 從最基礎的 OTP、PUF，逐步發展到 PUF Root of Trust。而現在，隨著 AI Server 對安全的要求愈來愈高，我們的技術又往前走了一大步，開始從單一的 Security IP，進一步提升到安全次系統，也就是 Security Subsystem 的設計與整合。

這個轉變對我們非常重要。

因為我們現在提供給客戶的，已經不只是 OTP、PUF 或 Root of Trust，而是進一步整合了加密技術、軟韌體，以及抗攻擊防護，形成一套更完整的系統級 Security IP。換句話說，我們在客戶晶片裡所扮演的角色變得更重要，能夠提供的價值也更高，因此每一個專案所帶來的授權金與權利金機會，也會跟著提高。

我們已經與多家國際記憶體大廠展開合作，把我們的 Security IP 導入到應用於 AI Data Center 的 SSD 系統，並提供符合 Caliptra 規範所需要的安全次系統。除了 SSD 以外，我們也進一步進入 AI Server 另外一個非常重要的領域，就是 Memory Expansion，也就是記憶體擴充。

AI 模型愈來愈大，AI Server 所需要的記憶體容量也快速增加，因此 CXL 正在成為 AI Server Memory Expansion 很重要的介面技術。而 CXL Switch 以及相關控制晶片，同樣需要完整的硬體安全架構。我們目前也已經和相關的 CXL 晶片公司合作，提供 Security IP 以及 Security Subsystem。

所以，如果我們把這幾年的發展連起來看，可以看到一條很清楚的軌跡。

去年，我們進入 AI / AGI CPU 與 BMC；今年，我們進一步拓展到 AI Data Center SSD、Security Subsystem；現在，我們又切入 AI Server Memory Expansion 所需的 CXL Switch。這代表我們的 Security IP 正從 AI Server 內部的單一晶片，逐步擴展到多個關鍵晶片。更重要的是，這些先進晶片有許多都採用 3nm 等先進製程節點，所帶來的授權金與權利金規模，可達公司平均水準的 10 倍以上。

另外一個對我們非常有利的趨勢，就是 Caliptra。

在 Microsoft、Google、Intel、AMD、NVIDIA 等國際大廠的共同推動之下，我們看到愈來愈多 AI 與 Data Center 的晶片和系統，開始採用 Caliptra 的安全架構。這代表未來需要 Root of Trust、Security Subsystem 以及相關 Security IP 的晶片會愈來愈多。因此，我們對 Security IP 在 AI Server 與 Data Center 的長期成長非常有信心。

接下來，我也要跟各位報告另外一個我們非常重視的成長機會，就是 Logic Flash。

目前，我們 Logic Flash 技術和晶圓代工廠的合作正在加速推進，而且應用不只是 Embedded Flash，也包括 standalone Flash 產品。我們認為，Logic Flash 的意義不只是增加一項新的 IP 技術。

更重要的是，它有機會利用更有競爭力的製程與成本結構，逐步取代部分現有的傳統 Flash 技術。Flash 本身是一個規模非常大，而且應用非常廣泛的市場。

因此，一旦 Logic Flash 開始進入量產，並逐步取代既有的 Flash 技術，它所能帶來的市場機會，以及對公司未來營收和獲利是深遠的影響。

所以，我們對未來多年的成長非常有信心。

接下來，我們請財務主管夏喬威先生說明 2026 年第二季營運報告。

營運報告

夏喬威，財務主管

第二季營運結果

各位股東，午安。

首先，我就先針對 2026 年第二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 10 億 9 仟 6 佰 6 拾 2 萬 7 仟元，較前一季成長 0.2%，比去年同期成長 17.1%。

在營業費用方面，本季營業費用為 4 億 3 仟零 5 拾 2 萬元，較上一季減少 0.3%，比去年同期增加 10.2%。

在營業淨利方面，本季營業淨利為 6 億 6 仟 6 佰 1 拾萬 7 仟元，較上一季成長 0.6%，比去年同期成長 22%。營業淨利率方面，較上季上升 0.2 個百分點為 60.7%，比去年同期上升 2.4 個百分點。本季淨利為 5 億 7 仟 9 佰 7 拾 9 萬 1 仟元，較上一季衰退 2.8%，比去年同期成長 44.9%。

總結，2026 年第二季的 EPS 為新台幣 7.77 元。

在總體營收中，我們分授權金及權利金來做說明：

1. 首先，第二季的授權金佔本季營收 39.2%，金額較上一季增加 12.8%，比去年同期增加 35.1%。
2. 在權利金方面，權利金佔營收比重為 60.8%，金額較上一季減少 6.4%，比去年同期增加 7.8%。
3. 2026 第二季的總營收比上一季成長 0.2%，與去年同期比較成長 17.1%。

以 2026 上半年來看，

1. 授權金佔上半年整體營收 37%，較去年同期增加 45.2%。

2. 權利金則貢獻了上半年整體營收 63%，比去年同期增加 7%。
3. 2026 上半年總營收與去年同期相比成長 18.5%。

第二季營收貢獻分析

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 21.9% 的總營收。本季授權金較上一季成長 11.2%，比去年同期衰退 22.4%。在權利金部分，NeoBit 較上一季成長 9%，比去年同期成長 9.2%。
2. **NeoFuse** 對本季的營收貢獻為 56.6%，較上一季成長 24.8%，比去年同期成長 55.6%。在權利金部分，NeoFuse 較上一季衰退 13.3%，比去年同期成長 4.4%。
3. **以 PUF 為基礎的 Security IP** 在本季貢獻 10.9%的營收。本季授權金比上季衰退 13.8%，比去年同期成長 133.5%。在權利金部分，比上季成長 213.9%，比去年同期成長 1676.7%。
4. **在 MTP 技術方面**佔總營收 10.6%。授權金比上一季成長 40.2%，比去年同期成長 9.3%。權利金貢獻較上一季成長 7.2%，較去年同期成長 19.2%。

在 2026 上半年，

1. **來自 NeoBit** 的授權金較去年同期衰退 18.5%，權利金成長 2.4%，佔 2026 上半年總體營收的 20.9%。
2. **NeoFuse** 授權金較去年同期成長 37.9%，權利金也成長 6%，貢獻了 2026 年上半年的整體營收 58.2%。
3. **以 PUF 為基礎的 Security IP** 授權金比去年同期成長 264.6%，權利金也成長 1317.8%，佔上半年整體營收的 11.6%。
4. **來自 MTP 相關技術**的授權金較去年同期成長 19.6%，權利金成長 30.4%，佔上半年整體營收的 9.3%。

第二季營收分析–Wafer Size

若以 8 吋及 12 吋晶圓區分：

1. **8 吋晶圓**權利金，佔第二季權利金營收的 37.5%，較上一季成長 4.2%，比去年同期

成長 1.2%。

2. **12 吋晶圓**權利金，佔第二季權利金營收的 62.5%，較上一季衰退 11.9%，比年同期成長 12.3%。

第二季完成的設計定案有 156 個，在 management report 中會詳細說明。

接下來，我們請徐清祥先生對未來展望做說明。

未來展望

徐清祥, 董事長

大家好，接下來我會向各位報告未來展望。

授權金方面：市場對先進製程技術、AI 相關應用、安全解決方案以及新世代 Flash 技術的需求持續強勁，帶動授權金持續成長趨勢。

權利金方面：權利金成長動能可望加速，主要來自於新增先進製程應用帶來的更高單價、新產品應用放量、PUF 權利金貢獻擴大，以及具較高權利金的 MTP 產品占比提升。

新 IP 技術進展

1. **先進製程 OTP 與 PUF-based 硬體安全：**持續針對 2nm GAA 及以下先進節點，開發驗證新世代 OTP 與 PUF-based 硬體安全解決方案，滿足客戶在裝置身份識別、金鑰保護、Secure Boot 與 Hardware Root of Trust 日益增加的需求。
2. **新世代 1T Flash：**1T NeoFlash 技術在嵌入式與獨立式應用持續推進；其相容標準邏輯製程的架構，可帶來更佳的擴充性、更低的製程複雜度與更高的成本效益。

商務平台擴展

1. **Chiplet Security 平台：**我們持續與生態系夥伴合作，為 Chiplet 系統建立端到端安全框架，涵蓋供應鏈可追溯性、身份識別與驗證、安全佈建、die-to-die 通訊、金鑰管理與 Hardware Root of Trust，以因應 AI、先進封裝與異質整合在地緣政治環境下日益複雜的安全挑戰。
2. **Data Center 安全與 Caliptra 平台：**針對資料中心與 AI Server 市場，我們將持

續深化既有客戶的加值銷售，把 PUFrt 從 Hardware Root of Trust 擴展為相容 Caliptra 架構的 Security Subsystem 與整合服務，降低整合複雜度並加速客戶導入。

3. **AI 運算與 Root of Trust 平台：**我們正將合作延伸至 CPU、AI 加速器與 AI ASIC 生態系，把晶片層級的 Root of Trust、Secure Boot、裝置身份識別與金鑰保護整合至新世代 AI 運算平台，強化從晶片到系統的信任與安全。
4. **HSM Edge Server 與 SECaaS 平台：**以 PUF 為核心的 HSM Edge Server 整合裝置身份識別、金鑰與憑證管理、Secure OTA 更新、簽章驗證、隱私保護與後量子密碼學（PQC）遷移。初期商機已在汽車 OTA、PKI 與 HSM 整合推進，並可望擴展至工業控制、Edge AI、智慧裝置、醫療與資料中心。
5. **Post-Quantum Security 平台：**我們持續強化 PUF-PQC 產品組合，開發具抗攻擊能力（含側通道防禦）的硬體安全技術，以支援邁向後量子安全標準的轉換。

以上就是我的報告。接下來，我把時間交給數位行銷主管徐浩先生，為各位分享我們今天的專題內容。

專題分享

徐浩，數位行銷主管

(Page 13: Securing the Next Generation of AI Infrastructure, the hardware anchor for Caliptra Root-of-Trust to secure Chiplets & CXL)

(Page 14: Introduction)

各位剛才在影片中看到的內容，其實只是圍繞 Caliptra 以及硬體信任根安全所形成的一個更大趨勢中的一部分。

在開始之前，我想先簡單說明這場簡報與我們最近參與的一些活動之間的關聯。本週稍早在台北，我們參與了 Caliptra workshop，內容聚焦在實作，以及如何讓規格更接近實際量產的矽晶實現。我們也參與了 OCP APAC 的兩場 session，從架構與系統的角度討論 Caliptra 與 chiplet security。

這些討論也再次印證了我們在產業中觀察到的一個更廣泛趨勢：隨著 AI server 與 data-center infrastructure 變得更加分散、也更加互連，這些安全技術的重要性正在

快速提升。

因此，今天與其試圖完整涵蓋 Caliptra 周邊正在發生的所有事情，我想利用接下來幾分鐘，聚焦說明這股趨勢正在加速成形的根本原因。而我想先從 AI compute 本身的改變談起，而不是從安全開始。AI 系統正愈來愈多地建立在多個 dies、accelerators、memory devices 與 high-speed fabrics 之上。當更多 components 被連接在一起時，這些 components 與 interfaces 也都需要被個別信任與保護。這正是今天這場專題演說背後真正要說明的主題。

(Page 15: AI Compute Can No Longer Scale in a Single Die)

當我們談到 AI compute 的擴展時，單純把一顆晶片做得更大，已經不再足夠。過去，如果我們想要更高效能，可以做出更大的 die，或移轉到更先進的製程節點。但這樣的做法已經面臨實際限制，包括 die size、yield、cost、power、memory bandwidth 與 I/O，都開始成為瓶頸。因此，產業愈來愈多地透過 composition 來擴展。

這張投影片中呈現了兩個重要的架構趨勢，我想先把它們區分開來，因為它們彼此相關，但並不是同一件事。

第一個是 chiplets，也就是在 package 內部運作的架構。與其打造一顆包含所有功能、非常龐大的 monolithic SoC，我們可以將系統拆分成多個具專門功能的 dies。例如，可能會有 compute 或 CPU die、負責 GPU 或 NPU 功能的 accelerator dies、I/O die、management die、security die，或其他 specialized functions。

非常重要的是，這些 dies 不一定需要使用相同的製程技術。Compute 的部分可能最適合使用最先進的節點，而 I/O、management 或 security 功能，則可能在較成熟的節點上更具經濟效益。因此，chiplets 帶來了模組化、重複使用性、更佳的經濟效益，也提供了另一種持續擴展 processor package 的方式。

但即使我們在 package 內部完成擴展，最終仍會遇到另一個邊界，也就是 processor socket 與 server 本身。這就是 Compute Express Link，也就是 CXL，開始發揮作用的地方。CXL 是在系統層級運作，位於 processor package 之外。

在這裡可以看到左側的 servers 透過 CXL fabric switch 連接到右側的 Type-3 memory shelf。記憶體不再永久只屬於某一個 CPU socket，而是透過 CXL 讓 memory 與其他 devices 能參與 coherent fabric。這代表 memory 可以逐步被擴充、pooling、共享，並在不同系統之間動態配置。

整體來說，我們可以這樣理解：chiplets 是透過在同一個 package 中組合多個 specialized dies 來擴展 processor；CXL 則是透過在 server 中連接 processors、accelerators 與 memory 來擴展 system。這對 AI infrastructure 來說是一個非常重要的轉變。我們正在從只依靠更大單一矽晶來擴展，轉向透過連接許多 specialized resources 來擴展。

但 composition 也帶來了安全上的後果。每一個新的 die、device、link、controller 與 firmware layer，都創造了另一個必須建立信任的位置。這也把我們帶到這個架構的另一面。

(Page 16: Composable AI Infrastructure Expands the Attack Surface)

同樣讓我們獲得彈性與擴展性的可組合架構，也創造了更大的攻擊面。這裡我再把它分成兩個架構領域來說明。

在 CXL 這一端，我們現在有多個 endpoint 加入 fabric，高價值的 memory 透過 link 傳輸，switch 控制連線，而 fabric manager 也可能決定 pooled resources 如何分配。這帶來了幾種不同類型的風險。例如，如果像 CXL switch 這類具有高度權限的基礎設施元件，其 firmware 遭到入侵，影響範圍可能會非常大，因為攻擊者鎖定的就不再只是單一 endpoint。他們可能進一步操控 fabric 中的連線、資源配置，或多個 device 的行為。

另一個重要領域是 DMA，也就是 direct memory access。DMA 本身是一項合法且非常強大的能力。安全上的問題在於，當遭入侵或惡意的 device 取得超過其應有範圍的存取權限時，如果這些權限沒有被妥善控管，device 就可能讀取或修改其授權區域以外的 memory。而在 memory 被 pooling 或共享的環境中，後果可能特別嚴重，包括不同 workloads 之間，甚至不同 tenants 之間的資料外洩。

在 chiplet package 內部，安全問題看起來不同，但原則是一樣的。現在我們面對的是多個 active dies 透過 die-to-die interfaces 彼此通訊。

假冒或惡意的 chiplet 可能把未經授權的元件帶入 package 或 supply chain，嚴重影響 silicon identity 與 supply-chain trust。惡意或未經授權的 die 可能植入 hardware Trojans、操控 transactions、外洩資料，或破壞整個 package 的安全假設。近年的 chiplet-security 研究也特別指出，惡意 chiplets 與 hardware Trojans 是重要的系統層級威脅。

Chiplets 也可能遭受攻擊，導致 key extraction 與 secret leakage。如果 root key 或 device secret 遭到破解，後果會遠大於單純遺失一筆資料。攻擊者可能得以假冒該 device，或破壞建立在該身份之上的信任關係。

我不期待大家記住這張投影片上的十二種攻擊方式，但重要的是它們共同告訴我們：trust boundary 已經擴大。安全不能再只存在於 board level，或只圍繞在 CPU 周圍。我們愈來愈需要知道的是：這個 device 或 die 是否真實可信？它是否啟動了可信任的 firmware？我能否信任其中的 keys？我能否信任 components 之間的通訊？以及，我能否向 system 的其他部分證明這份信任？

這就是為什麼 root of trust 愈來愈需要靠近個別 silicon 本身。而這也正是 Caliptra 這類架構變得非常重要的地方。

(Page 17: Caliptra Root of Trust Requires a Physical Security Anchor)

Caliptra 為現代裝置建立 hardware Root of Trust 提供了一套開放架構。但這裡有一個重要區別，也就是數位的 Root-of-Trust 架構，與其下方的實體安全基礎並不相同。

在左側，我們看到 Caliptra subsystem。Caliptra core 包含 RISC-V processor、cryptographic functions、SRAM 與 ROM、mailbox，以及負責實作安全架構的 firmware。但歸根究柢，所有這些數位安全邏輯，都必須錨定在 silicon 中某種實體基礎之上。

我希望大家記住三項基礎需求，我們也稱之為 foundational security primitives。第一，是 unique device secret（UDS）。我們需要某種對單一 silicon 個體而言獨一無二的資訊，用來建立 device identity 並支援 key derivation。第二，是 secure non-volatile storage。Security-critical information，例如 lifecycle state、configuration、seeds 或其他 protected values，必須能在斷電後仍保留下來，並且避免遭到未經授權的修改。第三，是 trustworthy entropy。這一層之上的所有 cryptography，最終都仰賴良好的 randomness。如果 entropy 很弱或可被預測，從中衍生出的 keys 也可能變得脆弱或可被預測。

因此，Caliptra 提供的是 Root of Trust 的架構與框架；但這份信任的基礎，仍然必須終止於 silicon 內部的實體特性與受保護狀態。這就是 physical security anchor。而這些需求，也很自然地對應到力旺與 PUFsecurity 多年來持續開發的 hardware security 技術。

(Page 18: PUFrt Provides the Physical Anchor Beneath Caliptra)

這裡我們就從架構走向實際的 silicon implementation。針對 unique device secret，我們使用 NeoPUF。NeoPUF 並不是單純把 root secret 寫入傳統 memory，而是從每一片 silicon 本身的內在實體特性中，衍生出裝置專屬的資訊。這為 device identity 與 key derivation 提供了與 silicon 綁定的基礎。

針對 secure nonvolatile storage，我們有 NeoFuse，也就是我們的 OTP 技術。NeoFuse 可為 security-critical information 提供受保護的儲存空間，例如 lifecycle values、seeds、configuration，或其他需要持續保存的 security assets。

針對 entropy，我們提供支援 TRNG 的實體 noise source，讓 cryptographic system 具備安全 key generation 與 operation 所需的 randomness。

而我們也透過 PUF-PQC，將這個基礎延伸到 post-quantum era。

重要的是，我們把這些 IP 視為同一個 security foundation 中的不同組成：identity、protected storage、trusted entropy，以及 cryptographic agility。這些能力結合起來，就是像 Caliptra 這樣的 framework 最終用來建立 trust 所需的 silicon-level primitives。但具備這些 primitives 只是問題的一部分。對客戶而言，下一個問題是如何把所有這些部分整合成一個完整且經過驗證的 security subsystem。

(Page 19: From Hardware Anchor to Security Platform)

這也正是我們的策略真正超越銷售單一 IP 的地方。我們以 PUFrt 作為 hardware anchor；在這個基礎之上，我們加入所需的 anchor IP、post-quantum security capabilities，更重要的是，加入我們與 Caliptra 相關的整合經驗。

因為從晶片設計者的角度來看，困難的問題不只是「我能不能授權一個 PUF？」真正的問題是：我要如何把規格轉化成真正能運作的 silicon？我要如何把 hardware primitives 連接到 Root of Trust 架構？我要如何驗證 interfaces？又要如何縮短整合與驗證時間？

這就是為什麼我們正朝向 validated subsystem 的方式前進。而一旦這個基礎建立起來，同一套安全架構就能擴展到 accelerator boards、AI servers、rack-scale systems，最終甚至延伸到 data-center infrastructure。

一開始只是 silicon 中幾個非常小的 security blocks，最終可以成為更大型 computing platform 的信任基礎。而這也讓我們回到一開始所談的，也就是這個愈來愈 composed 的 AI system。

(Page 20: Trust Must Extend Across Every Layer of AI Infrastructure)

AI infrastructure 正變得分散在多個層級之中。在 system level，CXL 可以透過 confidentiality、integrity 與 replay protection 等機制，保護透過 link 傳輸的資料。但保護 link，並不代表另一端的 device 就自動值得信任。那個 endpoint 仍然需要具備 identity、trusted firmware 與 secure boot，也必須能夠透過 attestation 證明自己的狀態。

Multi-die package 也遵循類似的原則：每一個 active chiplet 都可能擁有自己的 identity、keys、firmware、lifecycle state，以及與 package 中其他 dies 之間的關係。

因此，信任愈來愈需要從 data center，延伸到 rack、server、device、package，最後一路延伸到個別 silicon。而這也正是我們 foundation IP 如此重要的原因。

像 NeoPUF、NeoFuse、我們的 entropy source，以及 PUF-PQC 這類技術，雖然在整體 AI system 中可能只是實體上很小的部分，但它們提供了一些最根本的安全特性：unique identity、protected state、trustworthy randomness，以及 cryptographic trust。PUFrt 將這些能力整合成 physical hardware anchor，而 Caliptra 則提供在其上建立 Root of Trust 的架構。

因此，隨著 AI compute 變得更加 composable、更加 distributed，我們相信安全也必須朝完全相同的方向發展：trust 也必須變得 distributed，但同時必須持續 anchored in silicon。這就是我們所看到力旺與 PUFsecurity foundational IP 所扮演的角色：提供 silicon trust foundation，讓 secure chiplets、secure CXL-connected devices，以及最終下一世代 AI infrastructure 得以實現。

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!