使用 Microchip CEC1736 Trust Shield 晶片作為 AI 伺服器信任根 (RoT)

作者：顏睿余　主任現場應用工程師

SMART | CONNECTED | SECURE
小百科

什麼是 CEC1736 Trust Shield？

CEC1736 Trust Shield 是 Microchip 推出的一款信任根安全晶片系列，專門用來保護系統在開啟和運行的過程中免受駭客攻擊。它就像一個「安全守門員」，確保設備從通電的第一瞬間開始就在可信的環境中運作。這個晶片非常適合應用在以下領域：

- 資料中心伺服器
- 電信與 5G 基礎設施
- 網路設備與物聯網 (IoT)
- 工業控制系統
- 高效能運算 (HPC) 與 AI 平台

為什麼需要 CEC1736？

隨著現代設備日益複雜，駭客攻擊的方式也愈加多樣化。如果惡意程式是在系統開機「前」就被植入，那麼即便系統開機後已有安裝加解密系統或相關防護，這些防護依然可能為時已晚，整個平台已被駭客控制，並威脅資料外洩或服務中斷。CEC1736 的作用就是：

- 驗證開機程式是否安全
- 即時監控資料傳輸，阻擋可疑行為
- 防止未經授權的韌體更新

簡單來說，它能讓你的設備「從第一秒開始就安全」。

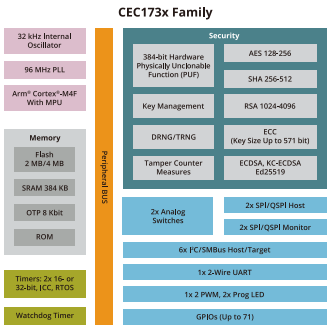
CEC1736 核心特色

CEC1736 不只是一款單純的被動安全晶片，它整合了多種技術，提供多種防護機制：

- **安全開機與更新**：確保只有合法的程式能啟動
- **即時監控**：檢查 SPI 與 I²C 等匯流排運作，防止惡意資料傳輸與破壞
- **PUF (Physical Unclonable Function) 技術**：每顆晶片都有獨一無二的「指紋」，難以複製
- **防駭設計**：包含旁路攻擊防護 (Side Channel) 及生命週期管理
- **強大加密能力**：支援 AES、RSA 和 ECC 等演算法，保障資料安全

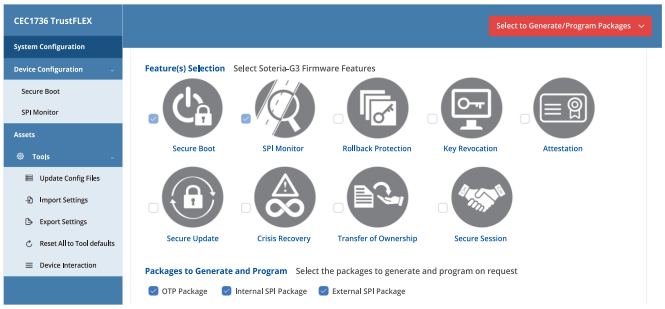
CEC1736 硬體規格簡單看

- **處理器**：Arm® Cortex®-M4F，核心時脈 96 MHz
- **記憶體**：4 MB Flash、384 KB RAM
- **安全元件**：PUF、OTP (防熔絲技術) 和不可變 Boot ROM
- **介面**：SPI、I²C 和 UART
- **封裝**：64 或 84-pin WFBGA



CEC1736 的優勢

- **符合國際安全標準**：NIST 800-193、OCP、TCG DICE 和 FIPS 140-2
- 通過第三方滲透測試，安全性有保障
- 搭配 Soteria-G3 韌體和 TPDS configurator 工具，開發快速、設定簡單



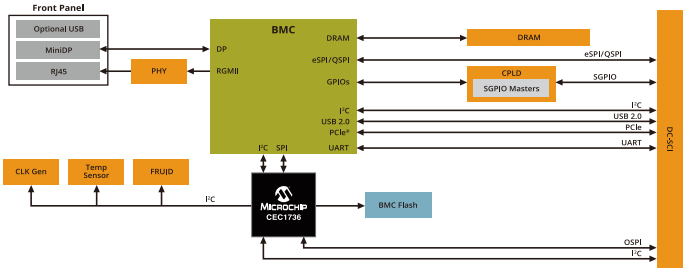
NVIDIA® GB200/GB300/B300/VeraRubin 應用案例

在高效能運算 (HPC) 與人工智慧伺服器中，安全性至關重要。以 NVIDIA GB200/GB300 NVL72、HGX B300，甚至於再下一代 Vera Rubin NVL144 的基板管理控制器 (BMC) 平台為例，這些系統通常需要從外部 Flash 啟動，並且必須確保 BMC 韌體與 BIOS 的完整性。CEC1736 在這樣的架構中，扮演著以下核心角色：

- **安全開機**：在伺服器啟動時，CEC1736 會驗證 BMC 與 BIOS 韌體是否為原廠簽署，防止惡意程式植入
- **韌體更新保護**：確保程式更新過程中不會被駭客竄改
- **即時監控匯流排**：檢查 SPI 與 I²C 資料傳輸狀況，避免未授權的存取
- **硬體信任根**：為 NVIDIA 平台提供符合 NIST 800-193 與 OCP 安全規範的防護

在資料中心部署 GB200/GB300 GPU 伺服器時，CEC1736 可與 BMC 搭配，形成完整的安全架構，確保整個系統從開機到運行都在可信狀態，這對 AI 訓練與雲端運算尤為重要。

請參考 OCP (Open Computing Project) 所提出的 DC-SCM (Data Center Security Control Module) 架構圖，CEC1736 即在其中擔任 RoT 的角色。



https://www.microchip.com/en-us/product/CEC1736-TFLX

https://www.microchip.com/en-us/development-tool/EV42J24A

聯繫信息 > Microchip 台灣分公司　電郵：rtc.taipei@microchip.com　技術支援專線：0800-717-718
聯絡電話：• 新竹 (03) 577-8366　• 高雄 (07) 213-7830　• 台北 (02) 2508-8600

MICROCHIP
SMART | CONNECTED | SECURE