專題報導

# 網路安全成熟度模型認證(CMMC)分享

資訊處網路工程課 洪韶謙

## 一、前言

CMMC（Cybersecurity Maturity Model Certification，網路安全成熟度模型認證）是一套由美國國防部（DoD）開發的框架，用於評估和增強美國國防供應鏈內企業的網路安全實踐。CMMC 目的是確保參與國防合約之企業具備足夠網路安全措施，用來保護**受控未分類資訊(CUI)**和**聯邦合約資訊(FCI)**。


## 二、CMMC 介紹

### CMMC 的背景

**1. 來源：**

- 隨著網路攻擊增多，美國國防部需要提出一套供應鏈內企業應有更強健的安全措施。
- CMMC 基於現有安全框架（例如 NIST SP 800-171 和 NIST SP 800-53），延伸引入認證要求。

**2. 目標：**

- 確保美國國防供應鏈中所有企業（包括主要承包商和次級承包商）都採取適當的網路安全措施。
- 將安全性與合約資格掛鉤：若未通過 CMMC 認證，企業將無法參與競標或執行 DoD 合約。

### CMMC 的關鍵要素

**1. 安全控制：**

CMMC 整合了多種框架（如 NIST SP 800-171）的安全控制，並將其分層為

不同成熟度級別(說明：NIST 800-171 美國國家標準與技術研究院（NIST）發布的一套資訊安全控制標準)。

**2.成熟度級別（基於 CMMC 2.0)：**

- Level 1: 基本網路安全

適用於處理 FCI 企業，需要符合 17 項基本網路安全實踐（對應於 NIST SP 800-171 第 3.1 類別)。

- Level 2: 進階網路安全

適用於處理 CUI 企業，需要符合 110 項安全實踐（對應於 NIST SP 800-171 全部安全要求)。

- Level 3: 專業網路安全

針對高風險國防計畫，要求額外安全措施和高級網路安全能力。

**3.審核與認證：**

- 企業需通過第三方審核機構(C3PAO)或自我認證（針對某些 Level 1 和部分 Level 2）來獲得 CMMC 認證。

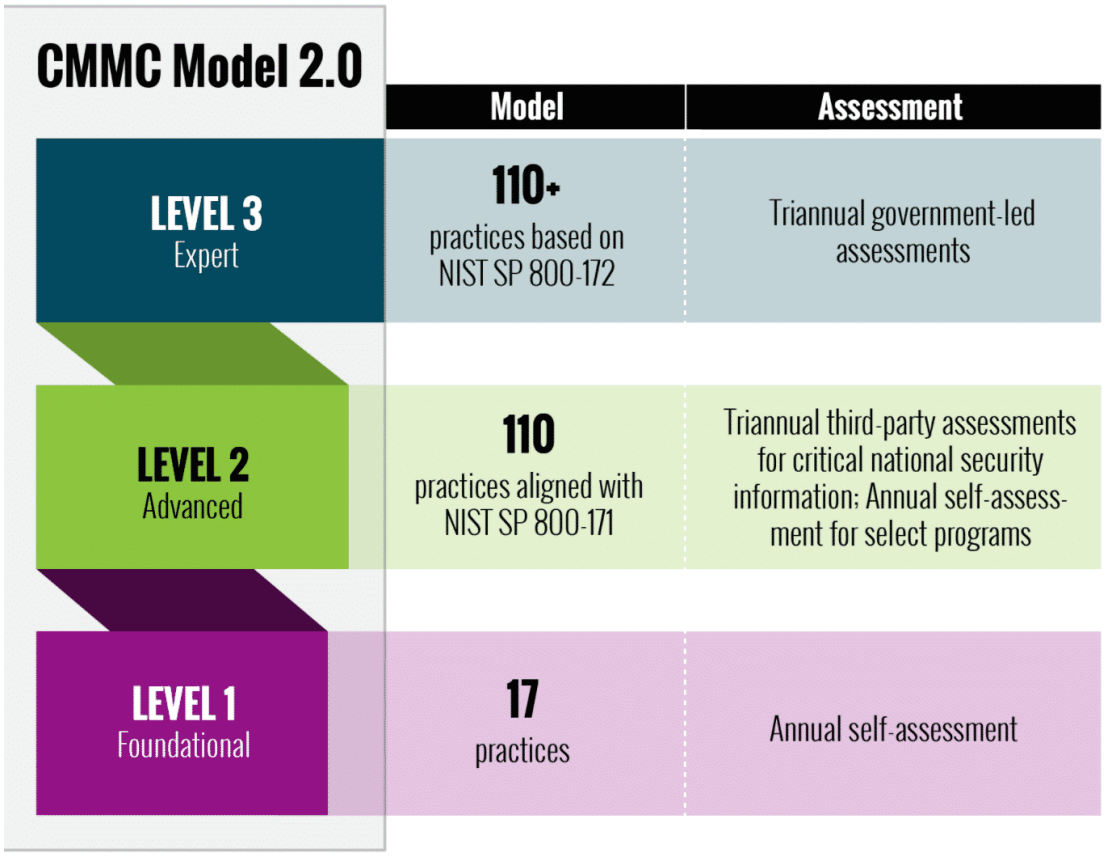



圖 1. CMMC 2.0 成熟度級別分級

## CMMC 的運作模式

**1. 合約要求：**

- CMMC 等級要求會在 DoD 合約中明確聲明。
- 企業需在投標前達到 CMMC 要求級別。

**2. 第三方評估：**

- C3PAO（CMMC 第三方評估組織）會根據 CMMC 框架評估企業的網路安全性。

**3. 持續合規：**

- 認證有效期通常為 3 年，企業需保持合規性得以繼續執行國防合約。

## CMMC 的意義

**1. 對國防部的意義：**

- 減少供應鏈中安全風險。
- 確保敏感資訊在供應鏈中得到保護。

**2. 對企業的意義：**

- 提升自身網路安全能力。
- 獲得競標 DoD 合約資格。

**3. 全球影響：**

- 雖然 CMMC 主要針對美國國防供應鏈，但其方法和標準對其他國家或行業別的網路安全是具有參考價值。



## CMMC 執行期程：

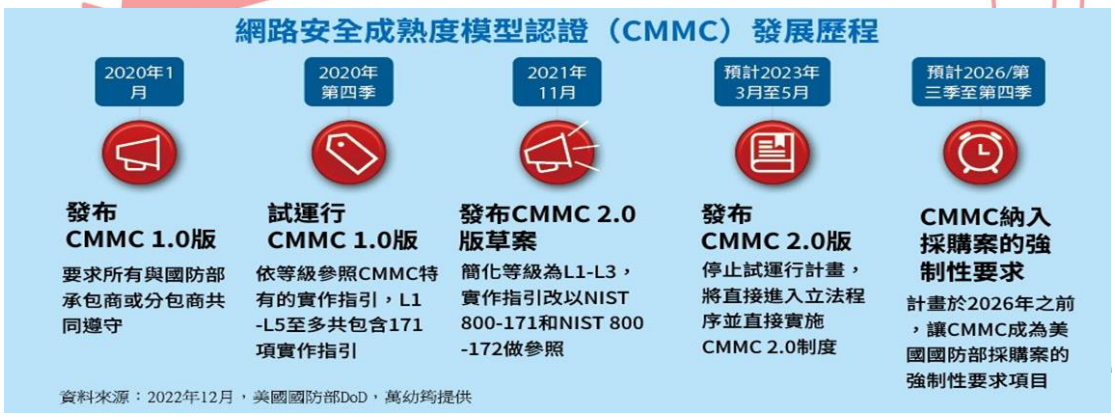



圖 2. 網路安全成熟度模型認證(CMMC)發展歷程

# 三、CMMC 對我國產業的影響

CMMC（Cybersecurity Maturity Model Certification）雖然是美國國防部針對其供應鏈推出網路安全標準，但對於台灣產業仍可能產生重要影響，特別是在以下幾個層面：

**1. 供應鏈參與**

台灣許多企業是全球供應鏈的一部分，尤其在高科技產業和國防相關製造領域（如半導體、電子製造與精密機械），若台灣企業涉及美國國防供應鏈或與美國國防承包商合作，可能需要符合 CMMC 要求。

- **具體影響：**
  - **出口限制：**未達到 CMMC 要求的企業可能失去向美國國防相關供應鏈出口產品或服務的資格。
  - **合約競爭力：**符合 CMMC 的企業將具有競爭優勢，特別是有美國國防相關的合約中。

2. **增加網路安全投資**

CMMC 要求供應鏈中的每個環節達到要求網路安全水準，台灣企業可能需要投入資金、人力和時間來符合這些要求。

- **具體影響：**
  - **技術升級：**需要實施符合 NIST SP 800-171 或更高標準網路安全技術。
  - **成本負擔：**企業需支付第三方審核費用、購買新設備、升級網路架構或僱用專業安全顧問。
  - **人力培訓：**增加對員工安全意識教育和技術培訓需求。



3. **產業競爭格局改變**

CMMC 實施可能改變台灣產業內競爭格局，一些中小企業可能因資源有限而無法滿足認證要求，進而失去相關市場機會。

- **具體影響：**
  - **大企業優勢明顯：**資源豐富大型企業更容易達到 CMMC 要求，進一步壟斷國防相關供應鏈市場。
  - **中小企業面臨挑戰：**對於資源有限企業來說，遵循 CMMC 要求可能是一項負擔，尤其是在 Level 2 或更高要求時。

4. **間接影響其他行業**

雖然 CMMC 主要針對國防供應鏈，但其影響可能擴展到非國防相關產業，許多跨國企業可能要求其供應商參考 CMMC 標準提升網路安全。

- **具體影響：**
  - **擴展到商業供應鏈：**隨著 CMMC 在美國國防產業普及，其他商業領域（例如航太、汽車、醫療設備）可能也會採用類似標準。
  - **台灣供應鏈壓力增加：**若客戶要求 CMMC 標準，台灣供應商必須主動調整，否則可能面臨訂單流失。

5. **政策與法規需求**

台灣政府可能需要因應 CMMC 的推廣，制定相關配套政策，幫助企業滿足全球市場的網路安全要求。

- **具體影響：**
  - **政府補助：**提供資金支持中小企業進行網路安全升級。
  - **法規調整：**加強台灣網路安全相關法規，使其與國際標準接軌。
  - **產業輔導：**建立專業團隊協助企業實現 CMMC 要求，提升台灣產業的國際競爭力。

6. **提升網路安全意識**

CMMC 引入可間接提高台灣企業對網路安全重視程度，進而減少資安事件風險。

- **具體影響：**
  - **改善企業形象：**通過 CMMC 認證企業將更具國際市場的信任感。
  - **降低資安風險：**實施更嚴格安全措施有助於防範資料外洩或網路攻擊。

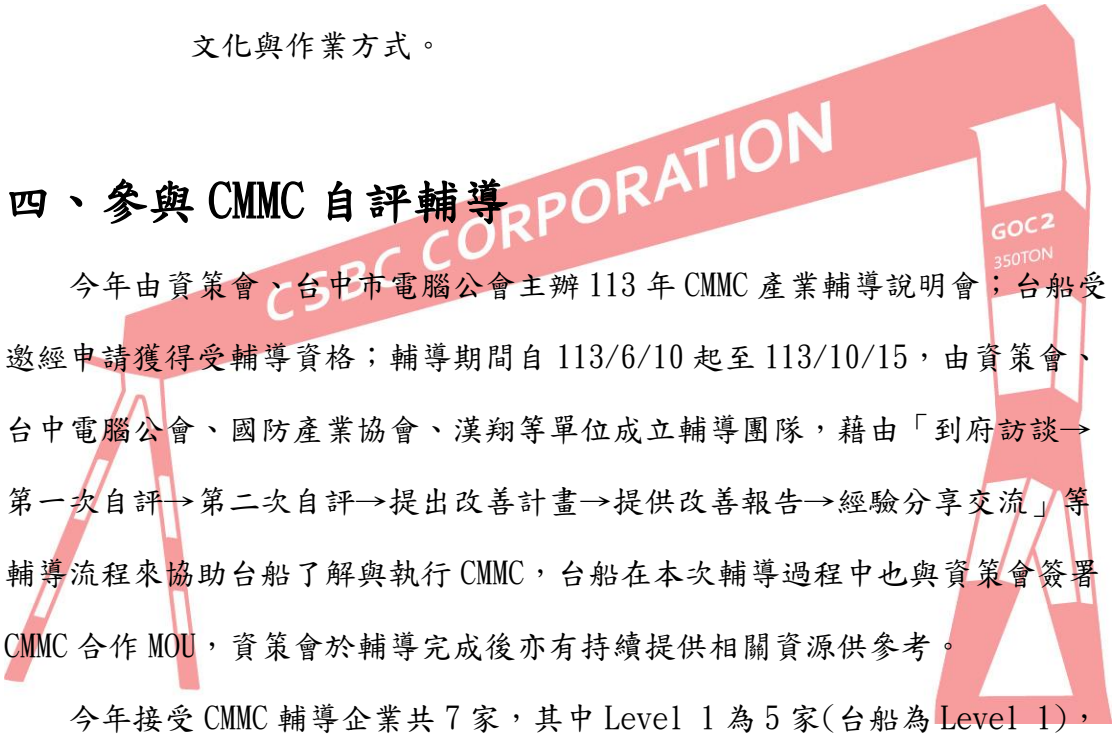
7. **長期機會與挑戰**

雖然 CMMC 實施對台灣企業會帶來短期壓力，但從長期來看，這也可能是一個機會。

- **機會：**

- **參與全球標準**：符合 CMMC 要求可提升企業競爭力，進一步參與全球供應鏈。
- **高端市場開拓**：進入具有更高安全要求的市場，例如國防、醫療和金融業。

- **挑戰：**
  - **實施成本高**：特別是中小企業可能需要政府支持才能實現符合規定要求。
  - **文化差異**：台灣企業需要適應美國對網路安全和符合規定要求的文化與作業方式。




## 四、參與 CMMC 自評輔導

今年由資策會、台中市電腦公會主辦 113 年 CMMC 產業輔導說明會；台船受邀經申請獲得受輔導資格；輔導期間自 113/6/10 起至 113/10/15，由資策會、台中電腦公會、國防產業協會、漢翔等單位成立輔導團隊，藉由「到府訪談→第一次自評→第二次自評→提出改善計畫→提供改善報告→經驗分享交流」等輔導流程來協助台船了解與執行 CMMC，台船在本次輔導過程中也與資策會簽署 CMMC 合作 MOU，資策會於輔導完成後亦有持續提供相關資源供參考。

今年接受 CMMC 輔導企業共 7 家，其中 Level 1 為 5 家(台船為 Level 1)，Level 2 為 2 家，受輔導企業多數為航太或軍工零件供應鏈相關產業。

漢翔分享導入經驗，漢翔自 105 年起開始做前置準備，於 108 年完成 110 項管制措施實施，於 112 年接受美國評鑑，成為台灣 CMMC 示範廠家，漢翔目前已是 F16 戰機後勤中心廠商，漢翔也要求其下游供應鏈要符合 CMMC 導入及符合規定要求作業，台船若要爭取美國國防訂單，提前準備以因應 CMMC Level 2 要求輔導供應鏈體系符合規定要求將是重要議題。


圖 3.113 年 CMMC 產業輔導分享交流會

## 五、結論

CMMC 是一個重要的網路安全框架，其執行標誌代表美國國防部對供應鏈安全高度重視，若企業參與美國國防供應鏈合約，需了解 CMMC 的要求並實施相對應安全措施，以確保符合規定要求並提高企業網路安全成熟度。

CMMC 標準對台灣產業既是挑戰也是機會。台灣企業應提早了解 CMMC 要求內容，特別是參與美國國防供應鏈相關行業，並積極採取相對應措施以提升自身網路安全能力，同時，政府與產業別應加強支援、協助讓企業在新的國際標準下維持良好的競爭力。