

採購規範書

1. 品名：模型上下文協定資安防護機制技術報告委託服務
2. 需求說明：為因應模型上下文協定（Model Context Protocol, MCP）應用快速發展所衍生之新型資安風險，本案將針對 MCP 應用之安全防護機制進行研析，包含 AI 模型與 MCP Server 間之工具呼叫、節點協作、權限控管、異常行為及攻防測試等議題，並探討結合 AI 智慧決策與既有資安檢測機制之可行架構及場域驗測方式，作為後續 MCP 應用安全驗證技術發展與導入之參考。
3. 規格/功能需求及交付驗收項目：

項次	執行項目	執行說明	交付/驗收項目
1	模型上下文協定資安防護機制技術報告	模型上下文協定資安防護機制研析相關主題： 一、AI + MCP 資安防護架構研析 研析生成式 AI 與模型上下文協定（MCP）應用之資安防護架構，包含 AI 智慧決策、MCP Server、資安檢測工具及相關系統間之整合方式。並針對工具呼叫、節點協作、權限控管及異常行為等可能衍生之安全風險進行分析，提出適用之安全防護與擴充架構建議。 二、MCP 安全驗證與國內外技術比較 蒐集國內外 AI、MCP 及自動化安全驗證相關技術發展現況，針對傳統資安檢測與 AI 智慧化安全驗證方式進行比較，並就自動化檢測、智慧決策、MCP 安全測試及多節點協作等面向，分析現有技術差異及後續發展方向。 三、AI + MCP 場域驗測規劃設計 依 AI + MCP 應用情境規劃安全驗測環境及驗證流程，研析節點資訊蒐集、輸入注入、未授權存取、權限提升等安全測試情境，並規劃測試執行、結果紀錄及風險分析方式，提出後續實驗場域或企業場域導入驗證之建議。	技術報告一式

2	其他配合事項	■ 廠商得標後，須與工研院召開會議討論技術方向及繳交研析項目細項，包括研究主題、預期技術內容，並供工研院審查與確認。 ■ 專案執行期間，應配合工研院提供除驗收報告外之相關分析與研析資料，並提供專案主題相關之技術顧問諮詢服務。 ■ 相關討論會議，不列入交付驗收項目。
---	--------	--

4. 交付驗收項目：

- 廠商於得標後須與工研院召開會議，討論技術方向及交付研析項目細項，並於115/11/30前繳交模型上下文協定資安防護機制技術報告一式，經工研院驗收確認合格後立即付款總額100%。

5. 廠商配合項目：

- 得標廠商需提供顧問諮詢，若有未詳盡事宜得標廠商得全力配合委託方進行補充。