政府科技發展中程個案計畫書

科技發展類前瞻基礎建設計畫

審議編號：114-1901-11-20-01

（國科會前瞻處、財團法人國家實驗研究院）

臺灣資安卓越深耕-學術型資安研究（5/5）

(核定本)

計畫全程：110 年 01 月至 114 年 08 月

中華民國 113 年 10 月

前後期別計畫內容修正對照表(A011)

前期(112 年-113 年)計畫名稱及經費審核情形：

臺灣資安卓越深耕-學術型資安研究

112 年度計畫名稱臺灣資安卓越深耕-學術型資安研究(3\5)

113 年度計畫名稱臺灣資安卓越深耕-學術型資安研究(4\5)

送審數 150,000 千元

核定數 135,000 千元

法定數 135,000 千元

前期(112 年-113 年)審查意見
1. 本計畫針對資安議題投入前瞻關鍵技術研究，規劃兩大分項計畫，包含前瞻司及工程司所推動之分項一 「前瞻資安技術研究」與前瞻司及國研院推動之分項二「資安科技擴散及共享服務」；針對未來在資訊科技上的應用情境，進行下一代資安技術研發。透過軟硬資安結合，提升資安防禦能量，了解並掌握目前科技前瞻技術與產業未來發展，也透過產業鏈結與強化國際合作關係，進而提升我國資安技術能量。
2. 分項一「前瞻資安技術研究」中規劃之研究項目，皆為當前重要資安技術議題，惟須注意細部議題是否與其他政府計畫題目重複，避免造成重複投資。分項二「資安科技擴散及共享服務」所規劃之「資安科技短中長期策略規劃」、「基礎資源整合與實證環境建構」 以及「育才與國際合作鏈結」等重點，皆明確可行。惟"雲端資安攻防平台"將提供學研甚至業界使用，除了應有的功能需求外，如何提供優良的使用者經驗，會是未來科技擴散及共享服務推展成功與否的關鍵，過去法人提出之平台不易使用一直常見的問題，建議本計畫應優化平台的使用性，並強化使用者意見回饋。
3. 本計畫為延續型計畫，計畫推動目標包含(1)軟硬結合、資安創新；(2)資安場域、淬鍊技術；(3)國際接軌、共同合作等。軟硬整合、場域技術、國際接軌與合作皆為國際資安科技發展趨勢與重點。本計畫目標與國際趨勢方向一致，規劃之計畫目標、預期關鍵成果 (OKR)、主要績效指標(KPI)大部分尚稱明確。但目標 3 國際合作部分除參與國際研討會發表論文篇數外，其餘產出不

明確，應予加強。綜觀 110 年度推動成果與目標達成情形，本計畫推動目標及運作應屬可行。但因本計畫 110 年度部分項目實際績效已達後續年度目標，故 112 至 114 各年績效目標應可予上調。

4. 本計畫所擬定之關鍵成果與目標扣合度高，惟部分成果屬於操作型指標展現，不易評估其執行品質。建議本計畫增加執行效益於預期關鍵成果中，以利展現推動成果與亮點。本計畫宜訂定資安人才培育品質及頂尖成果發表之評估機制，以強化本計畫相關推動之成效。
5. 政府已經投資多年 CDX 攻防場域，本計畫 CDX 攻防場域需要接軌國際趨勢（如 MITER ATT&CK）外，更應強化與國內資安產業或資安社群（HITCON 或 TDOH）合作，以驗證攻防平台是否達到國際等級。 如既有平台轉型不易，可改採民間替代方案。
6. 本計畫為「臺灣資安卓越深耕」主軸計畫之一環，協助發展學術型資安研究，完備 DIGI+及六大核心戰略產業創新方案資安能量。本主軸計畫所涵蓋五個計畫各有其短中長期任務，建議本計畫與其他計畫間強化水平互動及垂直鏈結，以達到整體計畫之綜效。
7. 本計畫所擬訂之自我挑戰目標中部分挑戰指標與 112~113 年度之預期關鍵成果相同，不具挑戰性，建議調整。因考量 110 年執行率未達 90%，經費應該有調整刪減空間。其中資安科技研究中心之籌組具有政策意涵，應優先予以經費支持。

序號	原計畫頁碼	前期(112 年-113 年)計畫內容（引原文或重點描述）	修正處頁碼	本期(114 年)計畫內容(引原文或重點描述)	修正原因
1					
2					
3					

…					

(114 年計畫內容無修正)

附表、前期(112 年-113 年)計畫細部經費配置

112 年

序號	細部計畫名稱	法定數(千元)	執行機構
1	前瞻資安技術研究(Security in Air & Security on Chip)	77,000	國科會前瞻及應用科技處、國科會工程技術研究發展處
2	資安科技擴散及共享服務	58,000	國科會前瞻及應用科技處、財團法人國家實驗研究院

113 年

序號	細部計畫名稱	法定數(千元)	執行機構
1	前瞻資安技術研究(Security in Air & Security on Chip)	77,000	國科會前瞻及應用科技處、國科會工程技術研究發展處
2	資安科技擴散及共享服務	58,000	國科會前瞻及應用科技處、財團法人國家實驗研究院

註：執行機構指受補助/委託之法人或學研單位(尚未執行可填「招標中」或「徵案中」)。

政府科技發展計畫書修正對照表(A009)

審議編號：114-1901-11-20-01

計畫名稱：臺灣資安卓越深耕-學術型資安研究（5/5）

申請機關(單位)：國科會前瞻處

序號	審查意見	計畫修正說明	修正處頁碼

(114 年計畫無修正計畫書之意見)

附表、計畫目標及預期關鍵成果之修正對照表(修正核定版填寫)

項目	送審版	核定版	
經費	送審數 114 年：75,000 千元	核定數 114 年：75,000 千元	修正說明
計畫目標及預期關鍵成果	目標 1: 軟硬結合、資安創新 關鍵成果 1: 針對開發前瞻創新資安防護技術促成產學合作。	目標 1: 關鍵成果 1: 關鍵成果 2:	無須修正
	目標 2: 資安資源共享與場域淬鍊 關鍵成果 1: 於資安科技研究中心召開專家會議研擬具突破性之尖端研究課題，並以 SaaS 服務架構整合資安軟體資源，提供數據服務及分析。 關鍵成果 2: 整合現有雲端資安攻防平台資源，彈性部署資安研發過程所需之測試並擴充弱點環境。	目標 2: 關鍵成果 1: 關鍵成果 2:	無須修正
	目標 3: 國際接軌、共同合作 關鍵成果 1: 強化與先進國家資安研發機構合作關係，提高國內資安技術水平。 關鍵成果 2: 積極展現臺灣資安實力，提升我國資安領域能見度，掌握國內外資安技術發展趨勢與領先地位。	目標 3: 關鍵成果 1: 關鍵成果 2:	無須修正

■請機關檢核確認業依審議通過之預算數及各項審查意見，妥適完成計畫內容修正(含計畫目標及預期關鍵成果修正) ■是 □否

目 錄

壹、基本資料及概述表(A003)

<table>
<tr><td>審議編號</td><td colspan="4">114-1901-11-20-01</td></tr>
<tr><td>計畫名稱</td><td colspan="4">臺灣資安卓越深耕-學術型資安研究(5/5)</td></tr>
<tr><td>申請機關</td><td colspan="4">國家科學及技術委員會</td></tr>
<tr><td>預定執行機關
(單位或機構)</td><td colspan="4">國科會前瞻及應用科技處、財團法人國家實驗研究院</td></tr>
<tr><td rowspan="3">預定
計畫主持人</td><td>姓名</td><td>陳國樑</td><td>職稱</td><td>處長</td></tr>
<tr><td>服務機關</td><td colspan="3">國科會前瞻及應用科技處</td></tr>
<tr><td>電話</td><td>02-27377530</td><td>電子郵件</td><td>glchen33@nstc.gov.tw</td></tr>
<tr><td>計畫摘要</td><td colspan="4">時代變遷與科技進步，IoT、5G、AI 等技術發展，使自駕車、無人機、智慧醫療、智慧零售、FinTech、智慧城市等自主系統應用日益普及；此些新興應用所採用的技術與機制相當複雜，因而產生許多潛在弱點；而駭客攻擊手法也從游擊戰，轉為具有策略、系統的團體戰，嚴重威脅我國邁向智慧國家的安全。有鑒於此，政府將「資安即國安」列為國家重大政策，「資安即國安 2.0 戰略」更著重提高人才培訓能量及開發資安創新技術；本計畫依循我國資安戰略，透過資安技術研發與機制設計，並培育資安研發人才，期能建立我國「資安自主研發」之厚實基礎。
計畫摘要中，本計畫規劃兩大分項計畫，包含前瞻處所推動之分項一「前瞻資安技術研究(Security in Air & Security on Chip)」與前瞻處及國研院推動之分項二「資安科技擴散及共享服務」，整合資安攻防平台與雲服務基礎設施之資源提供給前瞻科技研發團隊運用；針對未來在資訊科技上的應用情境，進行下一世代資安技術研發、培育資安技術研發人才與藉由產學合作及技術移轉擴散資安研發能量，帶動國內資安產業技術升級；同時，透過移地研究、舉辦與參與國際會議與社群活動，掌握國內外資安技術發展趨勢與領先地位，鏈結與強化國際合作關係，以利提升我國資安技術水平。</td></tr>
<tr><td rowspan="3">計畫目標、預期關鍵成果及與部會科技施政目標之關聯</td><td colspan="3">計畫目標及預期關鍵成果
114 年度</td><td>與部會科技施政目標之關聯</td></tr>
<tr><td colspan="3">目標 1: 軟硬結合、資安創新
關鍵成果 1: 針對開發前瞻創新資安防護技術促成產學合作。</td><td>國家科學及技術委員會:2:深耕基礎卓越研究，推動研發成果創新價值</td></tr>
</table>

<table>
<tr><td></td><td>目標 2: 資安資源共享與場域淬鍊
關鍵成果 1: 於資安科技研究中心召開專家會議研擬具突破性之尖端研究課題，並以 SaaS 服務架構整合資安軟體資源，提供數據服務及分析。
關鍵成果 2: 整合現有雲端資安攻防平台資源，彈性部署資安研發過程所需之測試並擴充弱點環境。</td><td>國家科學及技術委員會:2:深耕基礎卓越研究，推動研發成果創新價值</td></tr>
<tr><td></td><td>目標 3: 國際接軌、共同合作
關鍵成果 1: 強化與先進國家資安研發機構合作關係，提高國內資安技術水平。
關鍵成果 2: 積極展現臺灣資安實力，提升我國資安領域能見度，掌握國內外資安技術發展趨勢與領先地位。</td><td>國家科學及技術委員會:2:深耕基礎卓越研究，推動研發成果創新價值</td></tr>
<tr><td>預期效益</td><td colspan="2">一、強化未來新興科技資安防禦能量，確保智慧國家資訊安全
投入新興應用軟硬體資安威脅防護前瞻研究，預備新型態威脅資安防護實力，深化高階資安研發人才的培育與產業資安防護能力，厚植我國資安自主研發能力，建構資訊安全環境，邁向智慧國家發展目標。
二、建構資安資源共享機制，完善資安科技學研環境
整合跨域資安能量，以形成「資安科技研究中心」為目標，結合產學研專家組成智庫，串連學研供給研究成果，滿足產業需求，提升國內資安產業研發技術水平，促進沙崙資安基地資安產業聚落與生態系的形成；建置資安工具軟體共享平台，提供科技研究過程所需之資安工具軟體，透過建構雲端環境中軟體即服務(SaaS)方式，支持科研過程所需之軟體工具，以提供數據分析、異常通訊行為分析、預警模式測試，加速科研成果之展現。
三、提升國際能見度，建立國際資安研發領先地位
積極爭取國際發表機會，展示臺灣資安實力，跨國攜手合作進行資安技術研究，汲取先進國家資安開發經驗，提高我國資安技術研發水平，挑戰開發全球領先資安技術。</td></tr>
<tr><td>計畫群組
及比重</td><td colspan="2">請依群組比重填寫，需有比重最高之群組，且加總須 100%。
□ 生命科技 ____ %　□環境科技 ____ %　■數位科技 100 %
□ 工程科技 ____ %　□人文社會 ____ %　□科技創新 ____ %</td></tr>
<tr><td>計畫類別</td><td colspan="2">■ 前瞻基礎建設計畫</td></tr>
<tr><td>前瞻項目</td><td colspan="2">□ 綠能建設　■ 數位建設　□ 人才培育促進就業之建設</td></tr>
</table>

<table>
<tr><td>推動 5G 發展</td><td colspan="5">□ 是　　■ 否</td></tr>
<tr><td>中長程個案計畫</td><td colspan="5">■ 是，中長程個案計畫名稱：臺灣資安卓越深耕–學術型資安研究</td></tr>
<tr><td>資通訊建設計畫</td><td colspan="5">□ 是　　■ 否</td></tr>
<tr><td>政策依據</td><td colspan="5">1. FIDP-20210206070000：前瞻基礎建設計畫(110 年修訂版)：4.6.7 臺灣資安卓越深耕-學術型資安研究
2. PRESTSAIP-01090201010000：六大核心戰略產業推動方案：2.1 以科專計畫研發 IC 設計檢測、5G 等防護技術與 AI 輔助偵防
3. NICSP-20210102020000：國家資通安全發展方案(110 年至 113 年)：2-2 深耕學術型資安研究</td></tr>
<tr><td>計畫額度</td><td colspan="5">■ 前瞻基礎建設額度</td></tr>
<tr><td>執行期間</td><td colspan="5">114 年 01 月 01 日　至 114 年 8 月 31 日</td></tr>
<tr><td>全程期間</td><td colspan="5">110 年 01 月 01 日　至 114 年 8 月 31 日</td></tr>
<tr><td rowspan="2">前一年度預算</td><td>年度</td><td colspan="4">經費(千元)</td></tr>
<tr><td>113</td><td colspan="4">135,000</td></tr>
<tr><td rowspan="11">資源投入</td><td>年度</td><td colspan="4">經費(千元)</td></tr>
<tr><td>110</td><td colspan="4">125,000</td></tr>
<tr><td>111</td><td colspan="4">125,000</td></tr>
<tr><td>112</td><td colspan="4">135,000</td></tr>
<tr><td>113</td><td colspan="4">135,000</td></tr>
<tr><td>114</td><td colspan="4">75,000</td></tr>
<tr><td>合計</td><td colspan="4">595,000</td></tr>
<tr><td rowspan="5">114 年度</td><td>人事費</td><td>48,750</td><td>土地建築</td><td>0</td></tr>
<tr><td>材料費</td><td>10,347</td><td>儀器設備</td><td>0</td></tr>
<tr><td>其他經常支出</td><td>15,603</td><td>其他資本支出</td><td>300</td></tr>
<tr><td>經常門小計</td><td>74,700</td><td>資本門小計</td><td>300</td></tr>
<tr><td colspan="2">經費小計(千元)</td><td colspan="2">75,000</td></tr>
</table>

<table>
<tr><td>部會施政計畫關鍵策略目標</td><td colspan="4">深耕基礎卓越研究，推升研發成果創新價值</td></tr>
<tr><td>本計畫在機關施政項目之定位及功能</td><td colspan="4">本會為政府推動科學技術發展的專責機關，以支援學術研究為主要任務之一，於此主軸計畫「臺灣資安卓越深耕」中，協助發展學術型資安研究，支持推動 DIGI+2.0 及六大核心戰略之資安政策。透過未來產業的在資訊技術上的應用情境進行下一世代資安技術的研發，並以資安科技研究中心串連研究成果，將臺灣資安學術發展推向國際。</td></tr>
<tr><td rowspan="7">計畫架構說明</td><td colspan="4">依細部計畫說明</td></tr>
<tr><td>細部計畫 1 名稱</td><td colspan="3">前瞻資安技術研究(Security in Air & Security on Chip)</td></tr>
<tr><td>114 年度概估經費(千元)</td><td>46,200</td><td>計畫屬性</td><td>基礎研究</td></tr>
<tr><td>主管機關</td><td>國科會</td><td>預定執行機構</td><td>國科會前瞻及應用科技處</td></tr>
<tr><td>細部計畫重點描述</td><td colspan="3">為了建立智慧國家發展之安全環境，本計畫以關鍵技術的研發為核心，透過未來產業的在資訊技術上的應用情境，例如：自駕車、無人機、智慧醫療、智慧零售、FinTech、智慧城市、晶片安全等議題，進行下一世代資安技術的研發。透過軟硬資安結合，提升資安防禦能量，了解並掌握目前科技前瞻技術與產業未來發展，透過產業鏈結與強化國際合作關係，提升我國資安技術能量，在分項計畫一的主要工作項目包含(1)開發軟體資安技術(Security in Air)，(2)開發硬體資安晶片(Security onChip)。</td></tr>
<tr><td>預期關鍵成果(請填寫此細部計畫之主要關鍵成果(至多 3 項))</td><td colspan="3">114 年預期關鍵成果：
1. 促成產學合作或技術移轉案 6 件或總金額達 300 萬以上。
2. 專利 5 件/全期程、論文發表引用 50 人次/全期程、國際間攻防平台發展趨勢與功能分析技術報告 4 份/全期程、先進國家移地研究 3 件/全期程或邀請國際頂尖資安專家來台演講 3 場/全期程。</td></tr>
<tr><td colspan="3"></td></tr>
<tr><td>細部計畫 2 名稱</td><td colspan="3">資安科技擴散及共享服務</td></tr>
</table>

<table>
<tr><td rowspan="4"></td><td>114 年度
概估經費(千元)</td><td>28,800</td><td>計畫屬性</td><td>基礎研究</td></tr>
<tr><td>主管機關</td><td>國科會</td><td>預定執行機構</td><td>國科會前瞻及應用科技處、財團法人國家實驗研究院</td></tr>
<tr><td>細部計畫
重點描述</td><td colspan="3">本計畫整合跨領域資安能量，由學術單位建立前瞻技術，法人與社群搭建橋樑，也需與產業夥伴合作進行技術落地，形成資安技術供給網路。故分項二資安科技擴散及共享服務，原本雲端資安攻防平台維運將整合至基礎資源實環境之運用，並同步進行以下三項重點工作，分別是「資安科技短中長期策略規劃」、「基礎資源整合與實證環境建構」以及「育才與國際合作鏈結」。</td></tr>
<tr><td>預期關鍵成果</td><td colspan="3">114 年預期關鍵成果：
1. 完成資安尖端研究中長期戰略規劃報告 1 份，並促使 15 組研發團隊使用整合軟體資源服務。
2. 推動 1 場 100 人以上全國性雲端資安攻防競賽活動。</td></tr>
<tr><td>前一年計畫或相關之前期程計畫名稱</td><td colspan="4">110-1901-04-20-05：臺灣資安卓越深耕-學術型資安研究(1/5)
111-1901-04-20-04：臺灣資安卓越深耕-學術型資安研究(2/5)
112-1901-04-20-02：臺灣資安卓越深耕-學術型資安研究(3/5)
113-1901-04-20-02：臺灣資安卓越深耕-學術型資安研究(4/5)</td></tr>
<tr><td>前期
主要績效</td><td colspan="4">1.強化未來新興科技資安防禦能量，110-112 年累計 368 項前瞻關鍵資安技術或機制研發進行中、擴大培育高階資安技術研發人才達 932 人。
2.完成雲端資安攻防平臺(CDX)建置，110-112 年整合軟體資源服務並辦理 54 場次資安培訓課程、累計 2,696 人次參與。
3.提升國際能見度，累計發表國際論文 275 件。(國際研討會:125 件、國外重要期刊:120 件、國外一般期刊:30 件)。
4.打造產官學交流合作平台，橋接未來科技研發與產業需求，累計促成 87</td></tr>
</table>

<table>
<tr><td></td><td colspan="5">件產學合作、3 件檢測與驗證服務與 2 件技術移轉，合計 92 件合作案共 7,856 萬。</td></tr>
<tr><td rowspan="5">跨部會署計畫</td><td colspan="5">□ 是 ■ 否 （若屬跨部會合作計畫，請續填說明。）</td></tr>
<tr><td>合作部會署 1</td><td></td><td>114 年度經費
(千元)</td><td></td></tr>
<tr><td>負責內容</td><td colspan="3"></td></tr>
<tr><td>合作部會署 2</td><td></td><td>114 年度經費
(千元)</td><td></td></tr>
<tr><td>負責內容</td><td colspan="3"></td></tr>
<tr><td>中英文關鍵詞</td><td colspan="5">資通訊安全、晶片安全、前瞻研究、人才培育、國際合作
security in air, security on chip, foresight research, talents cultivation,international collaboration</td></tr>
<tr><td rowspan="3">計畫連絡人</td><td>姓名</td><td>李丹容</td><td>職稱</td><td colspan="2">科員</td></tr>
<tr><td>服務機關</td><td colspan="4">國科會前瞻及應用科技處</td></tr>
<tr><td>電話</td><td>(02)2737-7982</td><td>電子郵件</td><td colspan="2">sandy1@nstc.gov.tw</td></tr>
</table>

註 1

- 年度目標應敘明計畫預定達成的最終結果，關鍵成果則說明了如何衡量年度目標是否達成，兩者之間須有嚴謹的邏輯關係。
- 為聚焦投入目標，建議不超過 5 個為原則、每個目標對應的關鍵成果，建議最多以 3 個為原則。
- 關鍵成果的撰寫方式可從思考將「目標」轉化為「如何完成」的表述切入，每個關鍵成果都很「關鍵」，一個關鍵成果不能完成，目標就不可能完成。
- 目標撰寫公式與範例
  - ✧ 建議公式：

What (回答要做什麼?)，Why(解釋為什麼要做)

[副詞]+動詞+[形容詞+名詞，[動詞+名詞]

  - ✧ 範例

目標=動詞+名詞 (例: 防堵非洲豬瘟)

目標=動詞+形容詞+名詞 (例: 打造旗艦產品)

目標=副詞+動詞+名詞 (例: 成功促進產品外銷)

目標=What(動詞+名詞)+Why(動詞+名詞) (例: 開發疫苗，強化流感防疫)

- 關鍵成果撰寫公式與範例
  - ✧ 建議公式：

How (如何做)，How much(實現什麼)

透過[措施]+實現[可度量的結果]

✧ 範例

1.關鍵成果=措施+可度量的結果

(例: 透過法規輔導，完成 4 件產品海外上市)

(例: 透過補助產學合作案，完成 4 件可進行試量產的產品開發)

(例: 透過補助，完成當年度流感疫苗開發與生產)

(例: 透過驗證場域建置，完成 4 件符合國際標準的產品試驗證)

2.關鍵成果=可度量的結果

(例: 所有養豬場未檢驗出非洲豬瘟)

- 好目標的特徵

✧ 明確的行動方向 (用動詞指明行動方向，不要用協助、參與、支持等責任不明確的動詞)。

✧ 責任範圍是可控的 (例如打造全球最好的產品，可能達不到)。

✧ 在指定週期內是可以完成的 (如「完成概念設計」是可以完成的，「打造優秀團隊」雖也可以完成，但需要由 KR 來界定有沒有完成)。

✧ 精簡。

- 好關鍵成果的特徵

✧ 符合 SMART 原則 (Specific, Measurable, Attainable, Relevant, Time bound)。

✧ 基於價值 (由過去「任務導向」轉為「價值導向」，比起過去列出過程產出，改列出「具有價值的成果」)。

是關鍵的（對完成目標而言是重要的，訂定時要思考為什麼要完成這個成果）。

附表、整體經費配置表

項目 機關	重點內容或 工作項目 1	重點內容或 工作項目 2	…	**小計**
機關 A	（請填寫金額）	（請填寫金額）	（請填寫金額）	
機關 B	（請填寫金額）	（請填寫金額）	（請填寫金額）	
機關 C	（請填寫金額）	（請填寫金額）	（請填寫金額）	
…				
合計				

註：跨部會合作計畫必填，其他計畫免填

本計畫免填。

附錄 - 最終效益與各年度里程碑規劃表

最終效益(Endpoint)與里程碑(Milestone)規劃	修正說明
最終效益： 1. 強化未來新興科技資安防禦能量，確保智慧國家資訊安全。 2. 打造產官學交流合作平台，橋接未來科技研發與產業需求。 3. 提升國際能見度，建立國際資安研發領先地位。	無修正。
110 年度里程碑： 1. 開發 10 項前瞻關鍵資安技術或機制，促成產學合作 15 件或技轉 3 件或總金額達 600 萬以上。 2. 培育高階資安技術研發人才 125 人、參與國際頂尖研討會發表論文 8 篇。 3. 完成 2 項產業場域研究與建置(Blue Team、 Red Team Offense)，發展資安人才培訓情境，辦理新興科技資安攻防實務人才培訓 90 人次。	無修正。
111 年度里程碑： 1. 開發 10 項前瞻關鍵資安技術或機制，促成產學合作 15 件或技轉 3 件或總金額達 600 萬以上。 2. 培育高階資安技術研發人才 125 人、參與國際頂尖研討會發表論文 8 篇。 3. 完成資安資源共享平台建置，整合系統、網路、應用程式與技術檢測工具 4 類資源。	擴大原有雲端服務功能，提供資安軟體、檢測工具服務，提供學研單位解決資源取得不易問題，亦避免重新投資。
112 年度里程碑：	國家資安策略盤整;辦理高峰會，驅動資安生態系。

最終效益(Endpoint)與里程碑(Milestone)規劃	修正說明
1. 開發 15 項前瞻關鍵資安技術或機制，促成產學合作案 15 件或技轉 3 件或總金額達 700 萬以上。 2. 年培育高階資安技術研發人才 125 人、參與國際頂尖資安期刊/研討會發表論文 10 篇。 3. 辦理 2 次資安產學研高峰座談。 4. 推動 100 人以上全國性雲端資安攻防競賽活動。 5. 完成資安尖端研究中長期戰略規劃報告 1 份。 6. 參與或主導大型跨國資安研究計畫 2 案。	
113 年度里程碑： 1. 開發 20 項前瞻關鍵資安技術或機制，促成產學合作案 15 件或技轉 3 件或總金額達 800 萬以上。 2. 每年培育高階資安技術研發人才 125 人、參與國際頂尖資安期刊/研討會發表論文 12 篇。 3. 辦理 2 次資安產學研高峰座談。 4. 推動 100 人以上全國性雲端資安攻防競賽活動。 5. 完成資安尖端研究中長期戰略規劃報告 1 份。 6. 參與或主導大型跨國資安研究計畫 3 案。	國家資安策略盤整;辦理高峰會，驅動資安生態系。
114 年度(8 月)里程碑： 1. 促成產學合作或技術移轉案 6 件或總金額達 300 萬以上。	國家資安策略盤整;辦理高峰會，驅動資安生態系。

最終效益(Endpoint)與里程碑(Milestone)規劃	修正說明
2. 專利 5 件/全期程、 論文發表引用 50 人次/全期程、國際間攻防平台發展趨勢與功能分析技術報告 4 份/全期程、先進國家移地研究 3 件/全期程或邀請國際頂尖資安專家來台演講 3 場/全期程。 3. 辦理 1 次資安產學研高峰座談。 4. 完成資安尖端研究中長期戰略規劃報告 1 份。	

貳、計畫緣起

一、政策依據

1. FIDP-20210206070000:前瞻基礎建設計畫(110 年修訂版)4.6.7 臺灣資安卓越深耕-學術型資安研究。
2. PRESTSAIP-01090201010000:六大核心戰略產業推動方案 2.1 以科專計畫研發 IC 設計檢測、5G 等防護技術與 AI 輔助偵防。
3. NICSP-20210102020000:國家資通安全發展方案(110 年至 113 年)2-2 深耕學術型資安研究。

二、擬解決問題之釐清

時代的變遷與科技進步，資訊科技與網路已成為各國關鍵基礎建設，關係國家競爭力根本和人民福祉。加上中美貿易戰影響全球經濟，工研院產科國際所指出，現在是發展「安全產業鏈」的重要契機，2019 年臺灣資安產業產值達新臺幣 437.3 億元，年增率 11.1%，預估 2020 年我國資安產值應可達成新台幣 550 億元的目標。

總統蔡英文上任後，即將「資安即國安」列為國家重大政策，全力填補我國在「資安機制」、「資安人才」、與「資安自主研發」的不足。因國內資安產業發展瓶頸主要在於市場規模太小，無法吸引專業人才投入，因此資安人員招募不易，資安廠商也難以在技術研發上深耕，試煉場域不足也無法提升服務品質問題，加上有越來越多的新型資安問題，如何防範並挑戰市場機會，需要有更多的學術研究預先投入，進行前瞻技術研究，並建置實戰淬鍊場域，透過產學合作提升我國資訊安全技術與人才能量，漸而帶動國內資安產業技術升級與生態系建立，確保我國智慧國家之資訊安全，提升我國資安能見度。

本計畫為鼓勵學研界針對資安議題投入前瞻關鍵技術研究，規劃兩大分項計畫，分項計畫一為「前瞻資安技術研究(Security in Air & Security on Chip)」，分項計畫二為「資安科技擴散及共享服務」，原本雲端資安攻防平台維運將整合至基礎資源實環境之運用，擬將額外推動「資安科技研究中心」運作，並同步推行以下三項重點工作，包含「資安科技短中長期策略規劃」、「強化科研所需之整合基礎資源」及「策略性國際合作」等。執行機構包含國科會前瞻處、工程處和國家實驗研究院。本計畫將整合產學研跨域軟硬體資安能量，發展對抗新型態攻擊之資安防禦技術，協助我國八大關鍵基礎設施，研發快速反應與防禦保護機制，提升產業資安防禦能量。建置資安攻防新興主題實測場域，促成資安攻防解決方案與新興智慧應用結合、發展跨域資安整體解決方案。

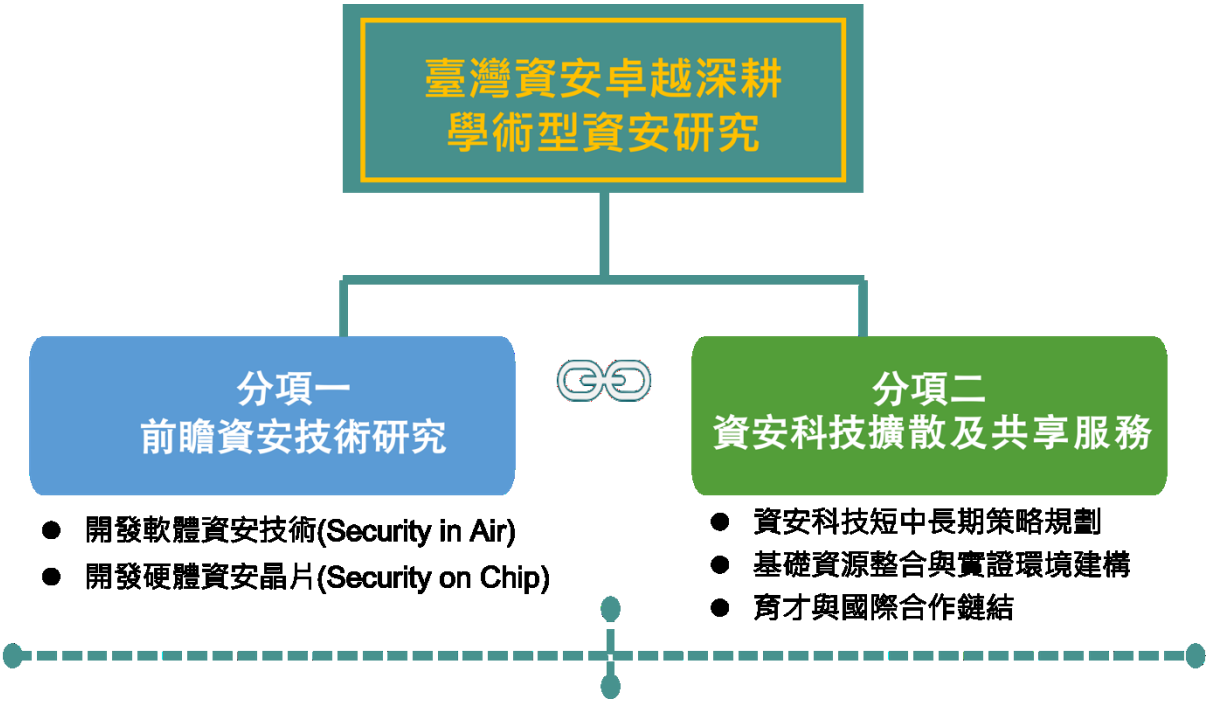

圖 1、計畫架構

為了建立智慧國家發展之安全環境，本計畫以關鍵尖端技術的研發為核心，透過未來產業的在資訊技術上的應用情境，例如：自駕車、無人機、智慧醫療、智慧零售、FinTech、智慧城市、晶片安全等議題，進行下一世代資安技術的研發。透過軟硬資安結合，提升資安防禦能量，了解並掌握目前科技前瞻技術與產業未來發展，透過產業鏈結與強化國際合作關係，提升我國資安技術能量，在分項計畫一的主要工作項目包含(1)開發軟體資安技術(Security in Air)，(2)開發硬體資安晶片(Security on Chip)，分項計畫二的主要工作為(1) 資安科技短中長期策略規劃，(2)基礎資源整合與實證環境建構(3) 育才與國際合作鏈結，以下將進行詳細說明。本計畫整合跨域資安能量，由學術單位建立前瞻技術，法人與社群搭建橋樑，也需與產業夥伴合作進行技術落地，形成資安技術供給網路。透過資安科技研究中心進行推動，運作架構如圖 2，工作項目與目標如圖 3。

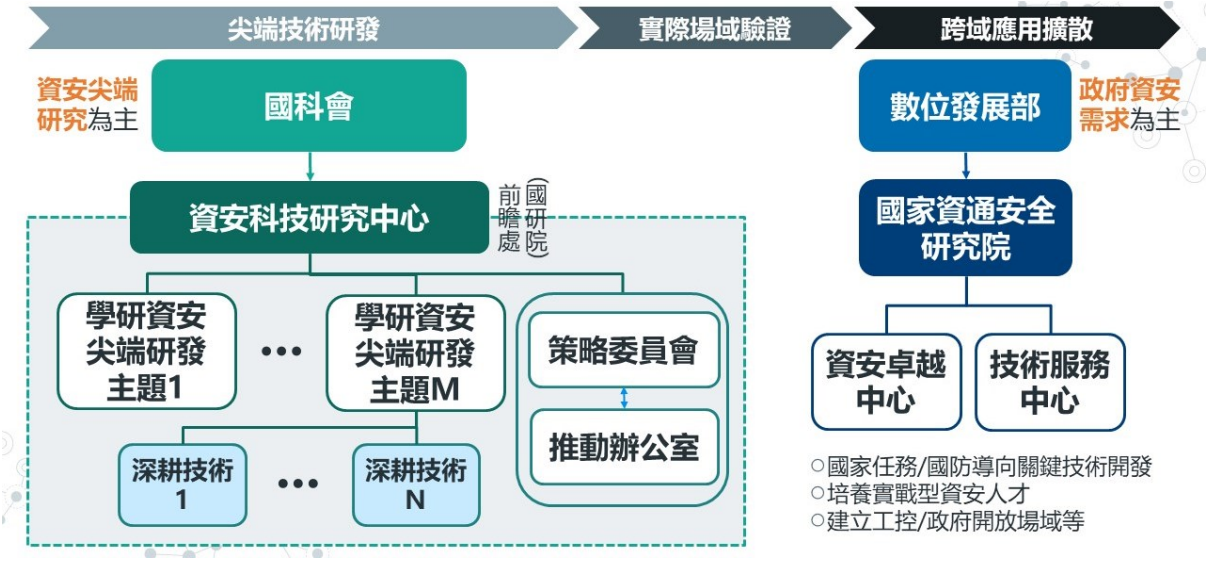

圖 2　資安科技研究中心運作架構

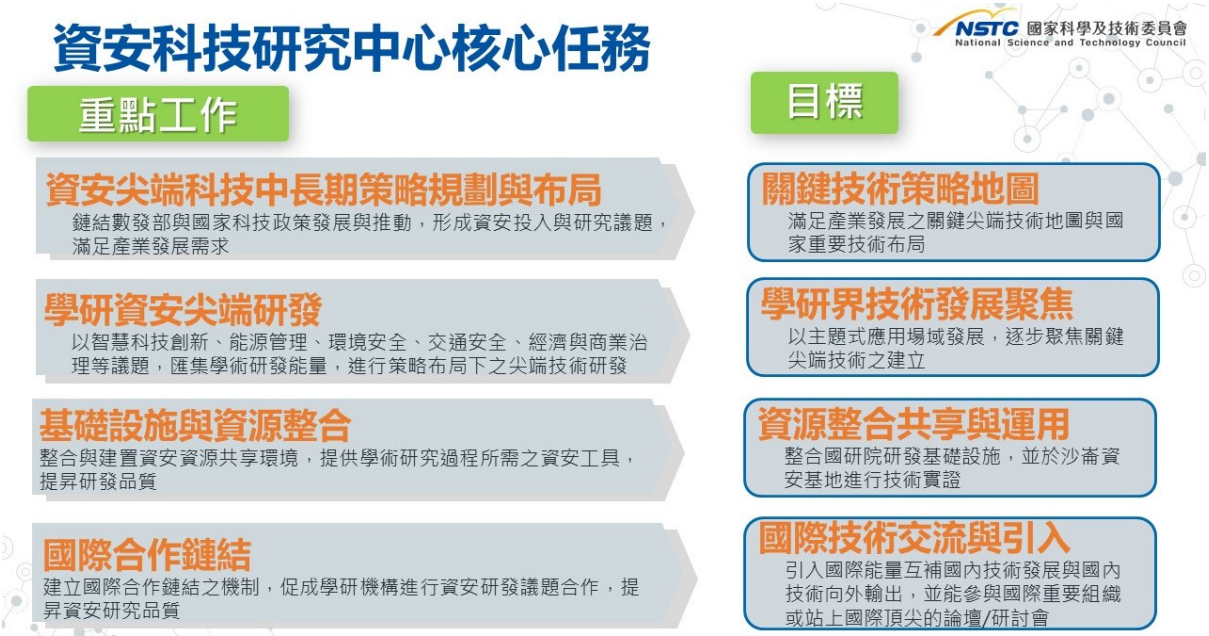

圖 3 資安科技中心核心工作與目標

分項計畫一「前瞻資安技術研究(Security in Air & Security on Chip)」

1. 開發軟體資安技術(Security in Air)

預期未來在 5G 商轉後，整合 IoT、5G 及 AI 的相關技術應用，會被國內的公、私部門大量採用，相關技術也會應用到關鍵基礎設施的管理系統上。同時，這樣複雜的整合應用，也會產生新興的資訊威脅，將阻礙我國邁向智慧國家的發展。本計畫將透過確認未來在 IoT、5G 及 AI 等公、私部門的應用情境下，如自駕車、無

人機、智慧醫療、智慧零售、FinTech、智慧城市等 IoT、5G、AI 等，可能會遭遇的資通訊安全問題，以及對關鍵基礎設施的資訊威脅，以研發與設計出下一個世代的前瞻資訊安全防護技術與機制。

當前 5G 位於起步階段，未來可以進行的商轉應用，除了提高當前 4G 應用的水準之外，也因為 5G 涉入雲端、行動裝置、車聯網等等領域，有可能會完全改變提供服務的軟硬體架構，各國對於 5G 資安防護的技術仍不成熟，是未來重要的資安議題。關鍵基礎設施的資安防護是資安議題的重中之重，隨著 5G 串聯 IoT 與 AI 新興技術與應用的出現，網路攻擊策略與技術也會不斷提升，對於關鍵基礎設施的資訊威脅也會不斷提升。AI 的技術現今已逐步融入日常生活中，如主動式行車安全防護、個人化推薦服務等，因此，未來除了利用 AI 進行網路攻擊的威脅之外，駭客攻擊 AI 系統讓 AI 系統癱瘓或是從而控制 AI 系統將會成為資訊威脅的重心。當新興技術不斷投入產業界，傳統的網路安全防護技術也將面臨技術升級的課題，例如如何讓資安人員看見這些看不到的攻擊、應用區塊鏈特質進行資料防護、自動化資安資訊或提高警示的準確率以降低分析人力的需求等。

在 Security in Air 部份下，包含 4 個研究項目，分別為：(1) IoT, 5G & Beyond 5G、(2) 關鍵基礎建設(油、水、電、金融等)、CPS 安全與工控、(3) AI 相關資安議題以及(4)網路安全(含區塊鏈等新興議題)，以回應上述未來我們即將面臨的資訊安全威脅，各項目詳述如下。

(1) IoT, 5G & Beyond 5G

第 5 代行動通訊（5th generation mobile networks, 5G）在通訊上具有 4G 所沒有的特性，也針對與物聯網技術以及人工智慧的應用，提出新型態的通訊方式、計算模型以及網路模型等，可支援更多開創性的應用。然而在未來的智慧 5G/B5G 的發展中，隨著各類智慧化終端裝置與邊緣計算裝置的數量大幅度的增加，異質性網路透過 5G/B5G 整合，使得資料分享的方式更為多元，以及因應應用而產生的計算需求也更為多樣化之下，產生了更多的資訊安全威脅以及防護的需求。

因應 5G 的蓬勃發展，目前已經有許多國家開始實際使用 5G 通訊，例如：韓國、美國、中國等國家，但也對應的衍生出許多問題和階段性不可避免的障礙和瓶頸。在 5G 的藍圖中，必須符合高頻寬、低延遲以及大量裝置連結這三項最主要的特性。以下就各國所遇到的情況大致以條列式進行簡單的國際現況之說明。

(1.1) 在高頻寬中，大部分國家所實際運行的 5G 系統都沒有辦法達到理想值 10Gbps 以上的速度，必須使用越高的頻率才能達到對應的速度，然而其

所能覆蓋的範圍則會相對的縮小，進而導致必須以更大量的天線來滿足需求，也導致部分國家之通訊供應商為了擴大支援的範圍會降低其訊號所提供的速度。

(1.2) 由於各國對 5G 也都僅僅是剛起步的狀態下，基地台和天線的部件尚非常稀疏， 僅僅是部分都市區域和較為核心的區塊能夠支援 5G，大部分的情況都還是會降階回 4G 的訊號，還甚至經常導致連線上的不穩定或沒有訊號。而目前參考文獻中有提到有對應方法可以主動將 5G 藉由基地台降階回 4G 的訊號，該部分也在 5G 的白皮書中也提到 5G 系統中會沿用 4G 的技術。這部分也會造成 5G 可能會產生 4G 原有的安全議題。目前期望除實現攻擊的部分，並朝向抵禦該攻擊為最終目標。

(1.3) 在大量裝置連結中，5G 涵蓋了大部分的日常生活應用，包括交通上的自駕車系統。然而，目前有文獻發現可以利用晶片中含有硬體木馬來影響自駕車輔助系統的判斷機制，此攻擊也會造成相當程度的危害並嚴重威脅到使用者的生命財產之安全。因此，未來目標將朝向偵測硬體木馬存在的演算法。

本計畫將依循國際主流的 5G/B5G 通訊標準如 GSMA、3GPP 或 ITU-R 等，進行 5G/B5G 之無線存取網路與通訊網路的安全機制、攻擊偵測與自我修復、基礎設施硬體安全、結合物聯網與人工智慧所需的安全計算方法，以及基於 5G/B5G 的應用與服務的安全， 並提出相關防護技術與安全機制。

(2) 關鍵基礎建設（油、水、電、金融）、CPS 安全與工控

國家關鍵基礎設施(Critical Infrastructure, CI)係指公有或私有、實體或虛擬的資產、生產系統以及網絡，此類設施倘因人為破壞或自然災害而受損，將影響政府及社會功能運作， 造成人民傷亡或財產損失，進而引起經濟衰退、造成環境改變，甚或使國家安全及利益遭受損害，因此世界各國政府均重視關鍵基礎設施之發展與建設。

自上世紀 90 年代以來，國際上數起重大天然災害或人為攻擊事件，均嚴重影響關鍵基礎設施之正常運作，諸如美國 1995 年奧克拉荷馬州聯邦政府辦公大樓爆炸事件、1999 年 911 恐怖攻擊事件、2012 年 Sandy 颶風，日本 2011 年東北大震災、2016 年熊本震災、2018 年北海道震災、燕子颱風、西日本豪雨、2019 年哈吉貝颱風等災害，均造成關鍵基礎設施受損嚴重影響各國之經濟民生。因此國際

間包括歐盟、加拿大、日本、澳洲等國， 對關鍵基礎設施防護的概念，已從實體設施防衛與保護，轉變為要求提升整體設施功能與系統的耐災韌性，並期在事故發生後能夠快速恢復與持續運作。因此，關鍵基礎設施的防護重點將不僅僅只是針對實體建築物與設備，若是從持續運作的角度來看，更包括關鍵技術與人員，及關鍵基礎設施之資通訊與監視控制系統等設施。

因此關鍵基礎設施之資安防護，已成為世界各國在強化關鍵基礎設施防護中不可或缺並快速成長之一環，例如水資源領域方面，2011 年美國伊利諾州公共用水系統遭攻擊，2015 年烏克蘭水力發電系統遭受攻擊造成數十萬戶大停電，2019 年委內瑞拉水力發電受駭客網路攻擊造成全國規模的大停電；金融領域方面，駭客集團企圖利用惡意程式攻擊全球逾 40 國家的銀行、電子支付系統與金融機構，估計已造成全球金融產業 10 億歐元的損失等，均顯示關鍵基礎設施資安防護之重要性所在。而就市場方面，Kenneth Research 於 2019 年 10 月研究報告指出，全球智慧電網資安市場規模在 2016 年為 44.5 億美元，預計 2025 年將成長至 110.6 億美元，更顯示關鍵基礎設施資安除為必要之環節外，同時亦有龐大之產業商機。

(3) AI 相關資安議題

人工智慧技術興起之後，AI 已經被企業大量用於商業營運中，在資訊安全領域也不例外，如利用 AI 的學習技術，針對進入本地端的惡意流量的 behavior group 進行分析與萃取，了解惡意流量的行為模式，明確地定義這些 behavior group 的演算方法，透過評估其分類演算方法的精準性，調整相關參數以達成良好的防禦效果。上述的 AI 技術，也被應用到數位鑑識的領域中，例如利用 AI 對端點設備的行為資料側寫進行分類與標籤，最後自動產生分析報告。

然而，AI 技術本身也並非不會遭受攻擊。若駭客有能力取得或是找到 AI 系統的運作方式，就可以透過資料的操弄，引導 AI 系統做出自己想要的結果。以自駕車為例，自駕車透過鏡頭收集行車影像(圖 4)，並利用 AI 的影像識別技術確認當前的車道、號誌、標誌等等，來決定行車的方向與速度。然而，當駭客知道車道、號誌、標誌的訊號強度後， 便能運用投影虛假的線條，讓自駕車誤判為車道從而影響車輛的行進方向。或是利用與標誌相近的符號或輪廓，讓自駕車誤判為速限標示，影響車輛的行車速度。

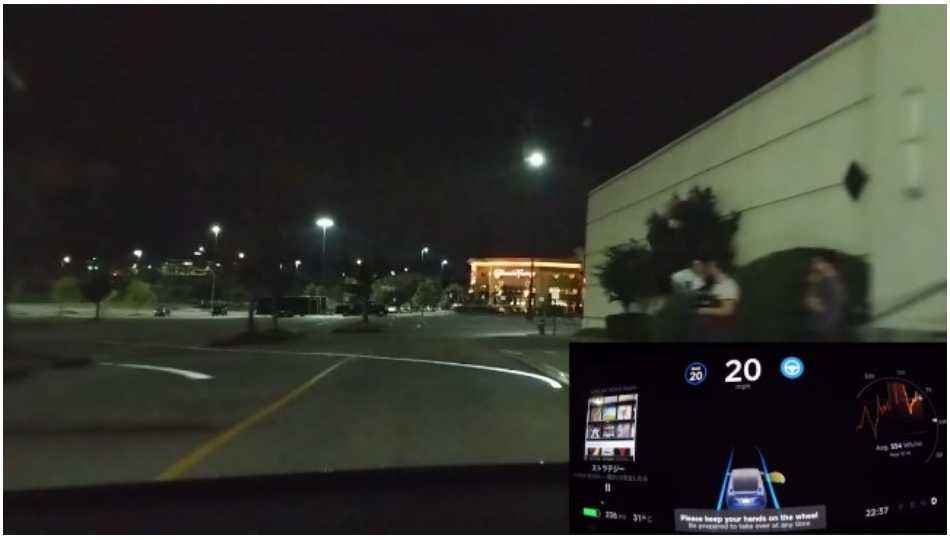

圖 4 誤導自駕車實驗

說明：研究人員利用在路面投影線條，成功影響自駕車行進的方向。資料來源：https://cyber.bgu.ac.il/how-a-300-projector-can-fool-teslas-autopilot/，Cyber@Ben-Gurion University of the Negev。

本計畫將著眼於 AI in Security 與 Security in AI 兩方面，一方面透過 AI 的技術，提升現有的資訊安全防禦技術的防禦率，以因應未來更為複雜的資安威脅。同時，對現有資安機制進行自主化，讓電腦能夠負擔大部分的人力工作，減輕資安人員的負擔，降低資安人力缺口的威脅。另一方面，發掘更多攻擊 AI 系統的威脅，並研發對應的防護技術或機制， 建立 AI 應用的安全環境。

(4) 網路安全(含區塊鏈等新興議題)

隨著 AI、5G、物聯網技術的推展，各式各樣的自主系統不斷出現，例如智慧工廠、自駕系統等。這些系統的組成複雜，操控訊號也會在不同的設備中移轉，現有網路安全技術必須能夠應付如此複雜的環境，才能確保自主系統的安全。舉例來說，自動化系統含有大量的程式碼，如 Chevy Volt 一千萬行程式碼、美軍 UAV 飛控軟體三百五十萬航程式碼、波音 787 有六百五十萬行程式碼，以及我們日常所使用的 Google 瀏覽器也有一百萬行之譜，因這些具有高度複雜性，所以不管是在設計階段、實作階段、或是營運階段皆有可能引入非預期的錯誤與漏洞。同時，AI 技術的快速興起，也讓駭客創造出更強大的惡意工具，如利用 AI 的技術，偽造主管的電子郵件或 CEO 的聲紋進行進行社交工程、繞過圖像驗證技術、大量掃描系統漏洞等，必須擁有相關資安技術，因應這些先進網路武器，才能降低 AI 攻擊的

資訊威脅。

區塊鏈發展也從加密貨幣的應用，逐步滲透至其他產業之中，例如食品業的食品履歷、福斯汽車的供應鏈管理計畫、加拿大鋼鐵溯源管理計畫、日本音樂版權協會的版權管理計畫等。作為新興的數位工具，區塊鏈也可以應用在 IoT 上，對 IoT 裝置進行探查、偵測、紀錄、側寫等行為，建立 IoT 的資安防護機制。然而，區塊鏈並非沒有資安問題，雖然區塊鏈的去中心化與共識演算法，確保了資料不被竄改的安全性，但是資料透明的特性，讓區塊鏈必須使用加密方法來確保資料隱私，成為隱私防護的課題。另一方面，智能合約是人為撰寫的程式碼，是極有可能產生區塊鏈漏洞的部分，如何才能建立或設計一套安全機制，來偵測或降低智能合約的程式錯誤，確保區塊鏈不要產生資安漏洞。

本計畫參考國際現況擬定未來研發主題(表 1)，透過開發新興資安技術，或是整合現有資安技術，全面提升網路安全的防護，以因應未來各種資訊安全應用發展。

表 1、軟體資安技術研發主題與國際現況

資安議題	議題探討
IoT, 5G & Beyond 5G	1. 各國對 5G 也都是剛起步的狀態下，資安防範皆不成熟。 2. 5G 涵蓋了大部分的日常生活應用，若被駭客攻擊會造成相當程度的危害。
關鍵基礎建設（油、水、電、金融）、CPS 安全與工控	1. 國家關鍵基礎設施若遭受駭客攻擊，將造成人民傷亡或財產損失，進而引起經濟衰退。 2. 國際就關鍵基礎設施資通訊安全技術及設備方面，仍多係以共通之工業控制系統。
AI 相關資安議題	1. 透過 AI 等技術進行網路攻擊偵測，駭客也開始利用 AI 等技術進行攻擊。 2. 電子系統邁向 AIOT 裝置，資安防範刻不容緩。
網路安全(含區塊鏈等新興議題)	1. 電腦犯罪手法日新月異且日益複雜，資訊資產不受到有意或無易地洩漏、破壞、假造，以及未經授權的獲取、使用、修改。 2. 透過區塊鏈系統本身的安全防護機制，或應用區塊鏈系統上的資訊安全防護機制。 3. 整合安全機制並擴展新興資安產業。

2. 開發硬體資安晶片(Security on Chip)

隨著時代變遷與科技進步，全球 IoT、AI 等技術快速演進與 5G 世代來臨，使現代生活發展趨向自動化及智慧化。根據市場研究機構 IHS Markit 預測，到 2025 年可連網裝置將超過 750 億台，如此大量的連接裝置可拉進人與人、人與物的距離，並提供更多管道搜集大數據資料，但便利同時也伴隨著隱憂，連接網路會讓這些裝置暴露在風險中，資安威脅大幅增加。由於這些新興應用採用的技術與機制相當複雜，因而產生許多潛在弱點與安全漏洞，讓駭客可能藉此入侵竊取個資或企業機密資料。近年各種資安攻擊事件時有耳聞， 對資訊安全的防護可說是未來科技發展所需克服的極大難題與挑戰。

關於資訊安全性討論方向主要可概分為軟體與硬體兩大類，近來各項新興技術應用對硬體安全性需求正高速增長。以目前蓬勃發展中的 IoT 應用為例，其架構涵蓋多種軟硬體整合， 包括晶片、記憶體、傳輸介面、通訊協定、應用程式及雲端平台等各種異質系統，若只利用軟體方式提供安全防護，已不足以防範層出不窮的資安威脅。之前揭露的 OpenSSL 旁通道攻擊漏洞就是一例，只要在附近用電磁波接收物理訊號，就可以獲得其加密金鑰；另外像是 2018 年 Nvidia 晶片漏洞禍及任天堂 Switch，以及近期造成熱烈討論的 Intel 與 AMD CPU 的安全漏洞等案例，皆是硬體安全議題最佳實證。據報導指出，單只 2018 整年就有超過 30 億各類系統晶片因硬體攻擊，遭受資料盜竊、綁架設備和其他安全性威脅。未受保護硬體可能威脅系統安全、可靠性和效能，讓廠商遭到財務和形象損失，甚至讓使用者暴露於危險之中，嚴重影響我國技術發展與資訊安全。

2019 年政府將「資安即國安」列為國家重大政策，加速研提「資安即國安 2.0 戰略」，顯示我國刻不容緩全力發展資安技術的決心。我國長期身為半導體設計與製造重鎮，上中下游產業鏈整合完整，擁有厚實的研發實力與提高技術在市場應用時效等多重優勢。爰此， 本計畫依循我國資安戰略，針對硬體安全防護技術研發，規劃「Security on Chip」主軸， 期能透過本計畫運作結合我國半導體產業優勢，加速關鍵技術研發進程，帶動國內資安產業技術升級與生態系建立，進而成為整體產業推動發展最堅實的後盾。

現今晶片設計與生產流程十分龐大而複雜，為增進效率，業界藉由全球化專業分工以降低製造成本，其過程至少牽涉到 IC 設計公司、設計自動化工具(EDA)供應商、矽智財供應商、設計服務公司、晶圓代工廠及封裝測試廠…等，每顆晶片都可能是全球不同公司團隊的合作結晶。晶片製作是一步步累積的過程，每個步驟都不能省略，高度化分工可以解決和減緩設計生產成本，但也讓安全議題浮出檯面。

換言之，IC 在設計或製造過程中都有可能被惡意改變電路、植入硬體木馬(Hardware Trojan)，或是管理不慎、機密外流、設計失誤等，都會造成整體安全漏洞，使每個步驟都可能面臨攻擊，成為重大資安破口。試將晶片開發過程參與廠商及各階段可能面臨之威脅(表 2)整理如下：

表 2 晶片開發過程及各階段面臨威脅

供應鏈相關廠商	晶片面臨之威脅
晶片設計者	IP 遭竊、機密演算法外流
元件 IP 提供商	外部 IP 安全性問題、遭植入硬體木馬
設計輔助工具/測試模擬廠商 (EDA/Simulation)	過度依賴 EDA 工具、工具可任意植入硬體木馬、扭曲規格限制造成其他運作條件外之不正常行為
輔助測試設計廠商 (Test-point/Test-pattern)	故意忽略邊界測試、特殊測試功能資料外洩
Gate layout (布局) 設計廠商	遭設計者植入硬體木馬、規則的晶片閘分布使逆向工程易於施作
晶圓代工廠 (FAB)	晶圓外流 (Overbuilding)
封裝測試廠	晶片外流
韌體設計者	安全協議設計錯誤、韌體安全漏洞、不當密鑰管理設計
韌體載入、參數設定、或機敏載入服務廠商	資料傳送過程外洩、密鑰外洩、邏輯疏失、測試不完備

除上述內容外，其他易受操弄的弱點還包含：

(1) CMOS 晶片耗電來自 0 與 1 變化，容易成為旁通道攻擊的主要依據。

(2) 非揮發性記憶體弱點，如 ROM mask 易於辨認、Flash 與 EEPROM 的耗電與資料殘留。

(3) 開發過程常留下接口以供往後除錯與監控，將成為安全漏洞。

(4) 晶片設計分工複雜，眾多人員參與以致設計原始資訊保密與管理不易。

(5) 冗長與複雜的開發流程使安全漏洞修補不易，面對威脅時難以快速回應。

為解決這些安全問題，本計畫將從晶片製造、晶片設計與架構等主題切入。在綜合考量目前國際現況、技術發展趨勢與成果效益等條件後(表 3)，我們訂定了後續推動策略方向，茲將相關內容簡述如下。

表 3、硬體資安晶片研發主題與國際現況

研發主題	國際現況
晶片製造	1. 內嵌 OTP (One Time Program)的密鑰，能防禦主動式攻擊，但無法防禦旁通道攻擊等被動式攻擊。 2. 晶片布局與非揮發記憶體，欠缺主動式遮罩(masking)，難以抵抗逆向工程。
晶片設計與架構	1. 所謂安全的軟硬體整合幾乎都在單一 TEE (Trusted Execution Environment)的開發環境且使用對稱性加密，密鑰管控困難。 2. 忽略邊界測試，所使用加解密 IP 僅防禦能量分析之旁通道攻擊，同時忽略 IP 竊取、植入硬體木馬等新式攻擊。 3. 即使是 Intel CPU 的晶片架構，也往往為追求硬體效能而衍生資安漏洞，尤其欠缺各式記憶體在執行程式時的保護機制與相關討論。

本計畫擬透過研發主題與國際現狀來擬定我國晶片安全未來方向，並擬定相關推動構面來強化我國硬體資安：

1. 透過 PUF 技術以加強晶片安全防護

物理不可複製函數（Physical Unclonable Function，簡稱 PUF）是目前用來產生晶片金鑰的最佳方式之一，可以當作是積體電路的「指紋」。其原理為基於積體電路中每個電晶體因為製程漂移而產生不同的物理特性，進而導致實際測量時不同電路的電子特性都有些微差異，而 PUF 正是利用這些在製造過程中不可控制的特性來產生獨一無二的金鑰；由於這些特性對製造商或攻擊者來說是無法被複製且不可預測的，所以 PUF 電路具備唯一性。

藉由 PUF 技術我們可以做到 Silicon IP 的保護、裝置認證以及金鑰產生；同時 PUF 無需在生產時載入金鑰，成本低廉，因此可安裝到大量的物聯網節點設備進而佈署於基礎設施中。除此之外更重要的是，相較於傳統方法，PUF 不需將金鑰儲存在硬體中，只有要用到時候才會產生，免除金鑰被竊取或攻擊的風險。種種優勢都讓 PUF 技術備受矚目，將之應用於晶片安全防護中也可顯著提高安全等級，如圖 5 所示：

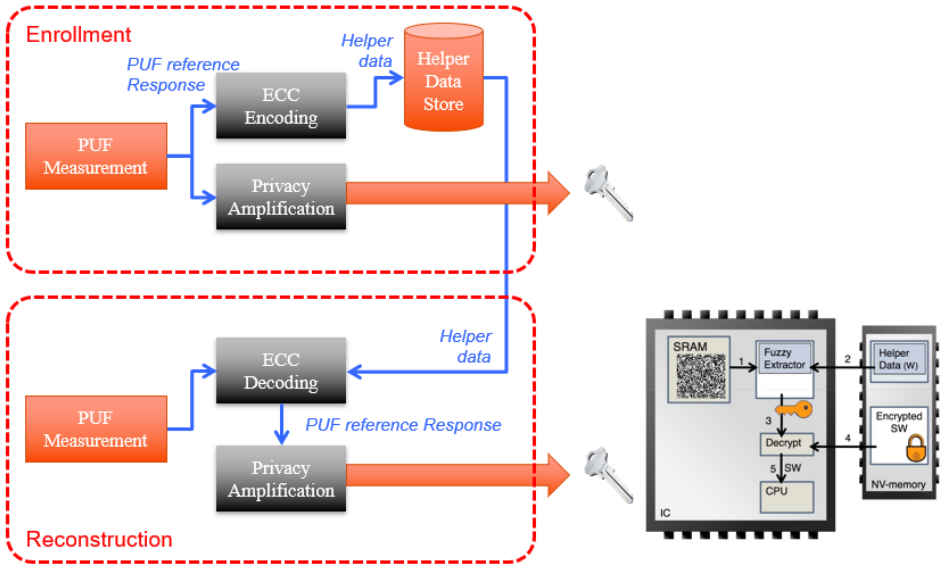

圖 5、應用 PUF 技術進行裝置認證示意圖

2. 基於安全設計的 EDA 工具與環境

電子設計自動化（Electronic Design Automation，EDA）是指利用計算機輔助設計軟體，來完成超大型積體電路（Very Large-Scale Integrated circuits，簡稱 VLSI）的架構設計、前端的合成與驗證，與及後端的電路佈局、繞線與規範驗證等實體設計。早期電路設計每個步驟與測試皆仰賴工程人員操作，然由於積體電路的規模日益擴大，絕大多數工作與步驟已被 EDA 軟體所取代，成為完成晶片設計不可或缺的工具，對設計品質與時程有重大影響。然而對 EDA 工具的過度依賴，倘若被有心人事植入惡意木馬、扭曲規格限制造成產生運作條件外之不正常行為，也使其成為晶片安全防護漏洞之一，對整體安全性構成重大威脅。

此外，隨著晶片開始擁有多樣化應用與感測、連結等功能需求，加上尺寸與功耗限制，大幅提升積體電路設計困難度，同時由於 2.5D、3D、小晶片（chiplet）等先進封裝技術實現之異質整合技術越來越受到關注，這也意味著傳統 EDA 工具已經無法滿足工程師們的需求。於此同時，因應前瞻晶片開發需求並注重安全設計的 EDA 相關技術，不論是在 IP 驗證或是前端與後端的 design flow，國內外皆十分欠缺；我國向來擁有厚實的半導體製造與晶片設計技術，如何據以帶動整體晶片設計與 EDA 領域發展，將是晶片安全的重要議題。

3. 旁通道攻擊防禦機制

旁通道攻擊主要基於從密碼系統的軟硬體實現中獲取資訊，例如：時間、功率消耗、電磁訊息甚或聲音等，皆可以提供額外資訊來源，並被利用於對系統的進一步破解。傳統加解密系統安全等級建立在數學模型上，金鑰長度決定破解複雜度，相應的攻擊演算法也是建立在數學模型漏洞中；但在實現加解密演算法的硬體架構，不同金鑰會產生不同的功率消耗、時間延遲、電磁波等物理特徵，這些洩漏的額外資訊，往往被有心人士利用而破解金鑰。

任何密碼演算法的軟硬體實作都會面臨旁通道攻擊，如何攻擊與相對應防禦機制的討論已經是近年來的資安領域顯學，更被稱為 CMOS 技術的宿命天敵。如圖 6 所示， 現今常見的實體裝置攻擊手法分析，就有至少 15%是來自於旁通道攻擊；目前針對加解密運算引擎如何防禦旁通道攻擊已有特別訂定 ISO 17825 國際標準作為參考規範，而過去國內學術界對於旁通道攻擊大多以功率消耗的分析與防禦為主，較少討論其他物理特徵的旁通道攻擊手法。因此，本計畫將推動更多業界廠商及學研單位投入研發，針對各式旁通道攻擊就對稱及非對稱演算法提出更完善的防禦機制，積極提高整體晶片安全防護能力。

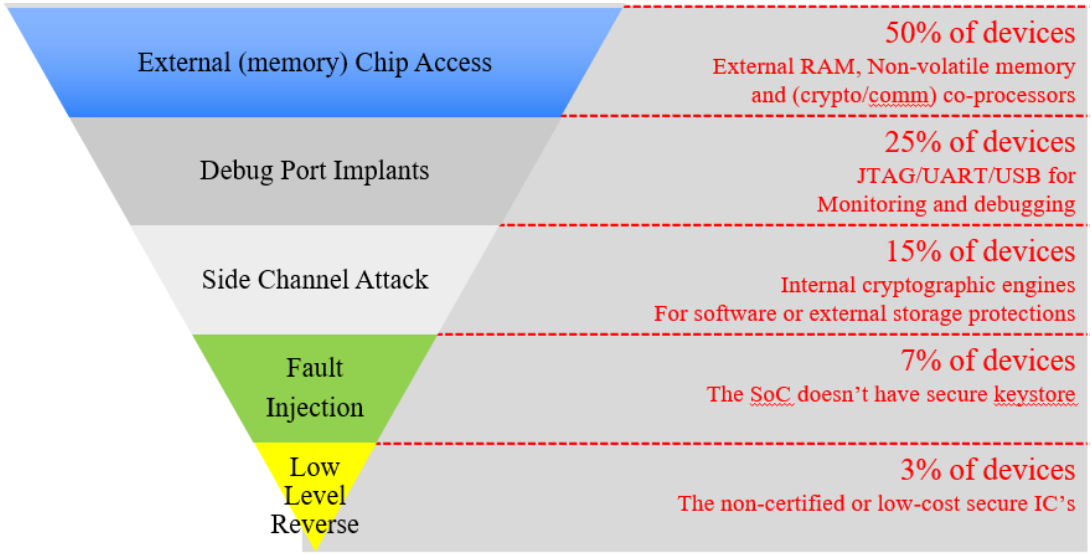

圖 6、實體裝置攻擊手法分析

4. 應用國際開源的晶片安全框架技術

可信任執行環境（Trusted Execution Environment，簡稱 TEE）在近年來是系統晶片（System on Chip，簡稱 SoC）安全的重要議題，其目的是將高安全敏感的應用與通用軟體環境進行隔離，藉以執行安全存儲、安全顯示等能力。目前 TEE 的國際標準由 Global Platform 組織來規範，標準中提供從開機啟動到後續執行軟體

的整套安全流程，將執行環境區分為可信任執行環境 TEE 及其他常用的系統環境（Rich Execution Environment，簡稱 REE）(圖 7)，其中 REE 如 Linux Android，TEE 則是獨立於 REE 之外的另一個世界，負責掌管系統機密的記憶體與執行機密程式的作業系統。在最新的規範中，也加入了更多考量，包含當系統中有多個 TEE 時，如何在應用層建立這多個 TEE 的互信關係。

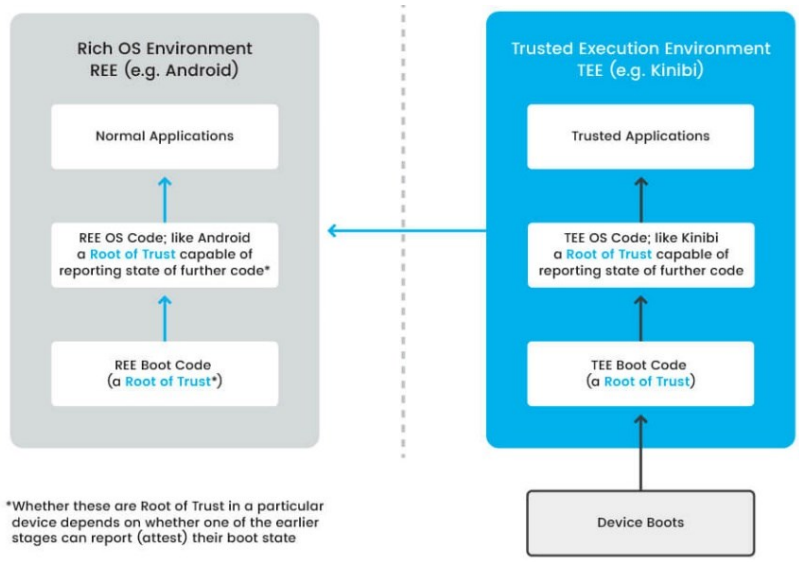

圖 7、可信任執行環境與其他系統環境

TEE 的系統規範中，硬體信任根（root of trust，簡稱 RoT）是個最關鍵的重要元素，主要指軟硬體元件裡無法被竄改、可以被完全相信的部分；用來確保元件在啟動時，是使用經過授權及驗證的程式碼。換句話說，RoT 實體是介於系統的啟動處理器和內含初始開機韌體的非揮發性 ROM 或快閃記憶體之間，在系統被允許啟動前，RoT 可以在處理器讀取韌體前驗證其完整性，如果潛伏的韌體 bug 可能產生某種威脅，RoT 還可以提供復原路徑。

值得一提的是，Google 近年開始執行 OpenTitan 計畫，目標是藉由更易取得且透明化的安全方案，讓開發工程師從系統 SoC 層級就能設計可信任安全性。未來 OpenTitan 專案將提供開放原始碼的晶片 RoT，包含公開韌體、指令集架構、SoC 架構、數位 IP、RTL 驗證與晶片包裝等(圖 8)。通過這些開源技術應用，將可簡化與加速晶片安全的整合開發。

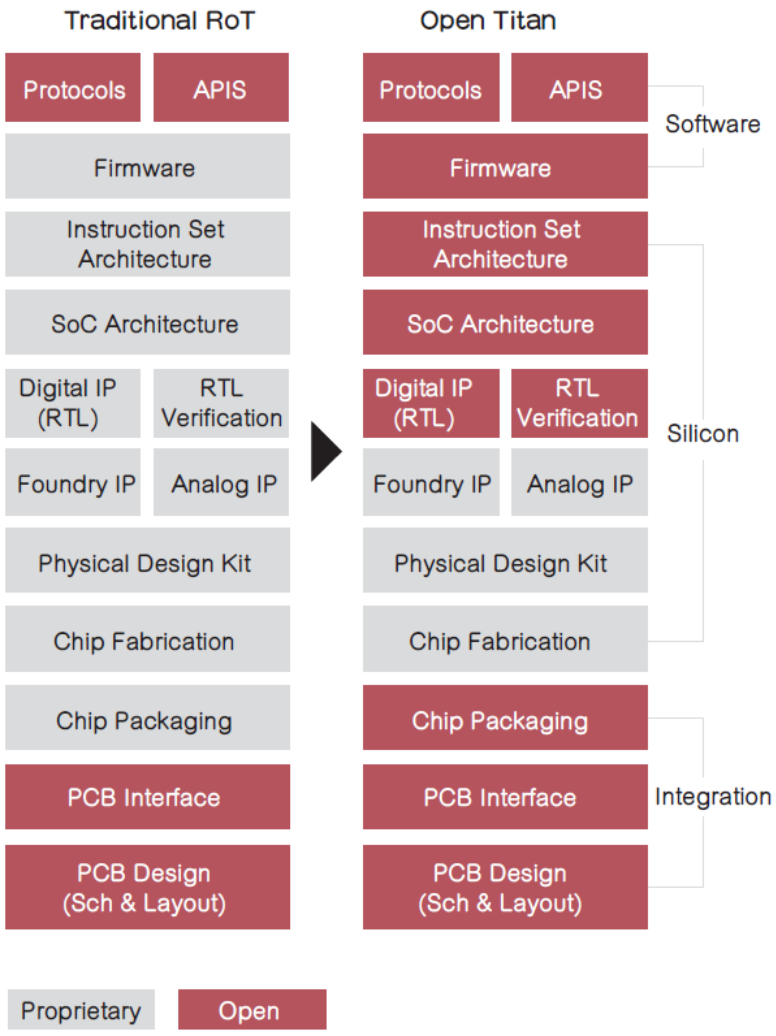

圖 8、傳統 RoT 與 OpenTitan RoT 主要設計比較

分項計畫二「資安科技擴散及共享服務」

本分項工作重點為除原本雲端資安攻防平台維運將整合至基礎資源整合與實證環境之運用之外、將額外推動「資安科技研究中心」運作，依下述 3 方向打造臺灣成為全球資安科研的關鍵夥伴。在中長期策略規劃與布局方面，由執行團隊盤整資安國際技術發展與應用生態，並以專家會議等方式收斂與聚焦頂尖資安技術與機會。經收斂的關鍵研究議題與發展方向將進一步由分項一的研究計畫執行，聚焦資安科技研發重點學校進行前端關鍵技術深耕，並擴大培育資安人才。於國際合作面向，由執行團隊透過資安科技研究中心品牌於國際積極爭取合作與發表機會，協助我國資安研究團隊競合全球資安應用領域，分別詳述如下：

圖 9、資安科技研究中心願景

1. 資安科技短中長期策略規劃

因應國家資通訊安全需求，資安議題已涵蓋各種資訊科技應用，國家層級資安科技發展，須長期進行規劃，本計畫透過「資安科技研究中心」布局策略規劃，並召開專家會議來研擬具突破性之尖端研究課題，訂定關鍵技術研發方向，續請分項一工作團隊依研究方向，展開分群組之研發工作，鼓勵專家學者投入此前瞻性的研發工作。

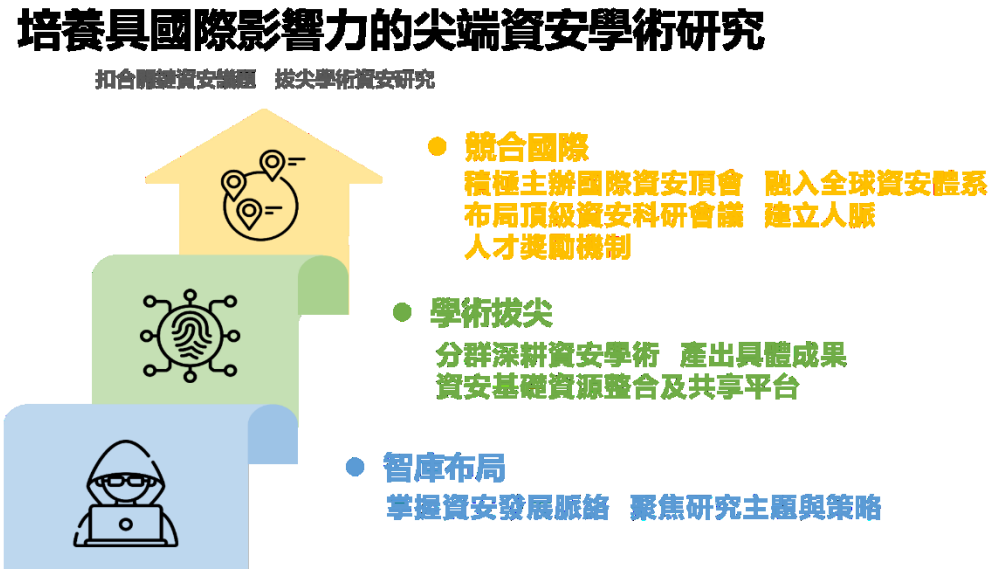

圖 10、資安科技研究中心布局資安中長期策略規劃

2. 育才與國際合作鏈結

由「資安科技研究」為核心，依前述策略規劃在各重點大學成立關鍵議題研究中心挑戰學術資安攻頂拔尖，進而提高臺灣資安科技前瞻影響力。此部分結合分項一關鍵議題之頂尖學者整合跨校研究群共同參與，將學研單位成果擴散並培育頂尖人才接軌國際，形塑國際級資通安全頂尖研究團隊：

(1) 挑戰學術資安攻頂拔尖：根據 Top down 選定關鍵議題，規劃與邀集研究團隊參與國際頂尖會議與活動，並以全球前 10 大期刊或研討會之研究成果發表為主要目標支持我國專家學者於國際頂尖期刊發表論文，融入國際科研生態體系，展現我國學術資安實力、累積研究能量，發表篇數逐年成長。鼓勵我國專家學者擔任國際重要資安會議主持人或主講人（keynote speaker）、代表我國於國際會議中提出合作倡議以及促成我國成為重要資安會議主辦國，以強化我國於資安領域之全球能見度與領導地位。

(2) 搭建國際科研合作平台：與主要國家之重要研究機構/單位建立、維持合作交流管道，例如美國國家科學基金會（National Science Foundation, NSF）產學合作研究中心（Industry-University Cooperative Research Centers, IUCRC）計畫項下之資安分析與自動化中心（Center for Cybersecurity Analytics and Automation, CCAA），透過資訊交流與經驗分享，逐步建立合作共識，對焦全球資安議題，策略引導研究團隊進行國際合作，貢獻臺灣能量。未來逐步建立臺灣資安研究合作品牌，延攬國際知名大師加入或指導研究團隊，進而臺灣能夠參與或主導大型跨國資安研究計畫。

(3) 培育頂尖人才接軌國際：建立跨國培育管道，透過國際科研機構合作窗口，協助資安人才短中期出國進修及交流，以提升人才國際視野。並邀請國外專家學者來訪，透過實質交流強化國際學術鏈結。再配合建立卓越團隊與成果獎勵機制，包括取得國際卓越成果(拔尖)之團隊或人才的鼓勵機制、高階人才持續深耕強化機制與鼓勵潛力新秀資安創新研究的機制，進而鞏固資安人才，孕育學研競逐尖端資安研究。

3. 基礎資源整合與實證環境建構

由基礎資源整合與實證環境建置應用而言，「雲端資安攻防平台」採用雲端虛擬化技術為基礎，改善傳統實體架構所面臨資源調配與環境部署耗費時間等問題，

並可彈性調配資源以部署資安研發過程所需之測試環境，透過實際場域的驗證，可進行研發方向與功能的測試。

(1) 雲端資安攻防平台服務方式

於資安科技研究中心整體策略規劃下，以 SaaS 服務架構整合資安軟體資源，提供數據服務及分析，提供 120 台虛擬主機供學研使用，及提供超過 150 種以上的弱點環境供研發團隊運用，並積極推廣研發團隊使用整合軟體資源服務。

(2) 雲端資安攻防平台功能特色

存取控制：由於平台提供許多資安相關工具，為避免遭到有心人士誤用，本平台導入完整的存取控制機制，透過帳號認證與權限控管，來進行使用者的管理。此外，為避免於資安攻防演練時，不慎影響內部網路使用者以及其他網路服務，雲端資安攻防平台之也搭配專屬的隔離網路環境，並進行更嚴格的存取規則管控。

快速部署：平台採用虛擬化技術進行建置，並搭配分散式儲存機制進行資料的存取，且具備節點高可擴充性的特性，因此可以更快的完成環境的部署。傳統架構下部署一間電腦教室的演練環境約需花費 30 分鐘，但於此平台部署僅需花費約 90 秒即可完成，對於需要大量增刪的資安實作環境來說，快速部署確實扮演相當重要的角色。

課程整合：平台與教育部資安人才培育計畫合作，協助進行客製化課程功能的開發，提供課程管理及上架功能，使用者可依課程模組內容規劃製作成單元，並綁定至不同的課程主題，同時亦可支援課程共享的功能，讓更多學校的教師可以使用該門課程進行教學推廣，協助培育國內資安實務型的人才，以因應未來產業界的資安人才需求。

競賽環境：可透過平台隨選弱點(Vulnerability On Demand, VOD)的功能，部署專屬個人或單位的競賽環境，亦可建置一套模擬企業網路架構的環境，搭配虛擬化資安設備及存在漏洞的對外服務系統，並採用紅軍及藍軍的攻防模式進行競賽，以驗證企業資安防禦架構的強度，並協助提升資安攻防的實務技術能力。

隨選漏洞：平台可提供超過 150 種以上的弱點環境，類型已涵蓋系統漏洞、應用程式漏洞、網站及資料庫漏洞、邏輯及權限漏洞…等等，使用者可以透過隨選弱點(Vulnerability On Demand, VOD)的方式，部署自己演練或培訓所需之環境，另外亦可提供多種不同的資安工具及環境，讓平台使用者可以快速使用，免於花費時間尋找及安裝。

資安教材：針對教育訓練學員提供資安相關教材，領域涵蓋 12 類以上資安技術，其中包括滲透測試、弱點掃描、惡意程式分析、網路封包分析、網站安全、數位鑑識…等等，並可搭配課程功能建置培訓所需之實務操作環境，協助學員提

升資安實務的技術能力，並將所學技術應用於日常工作維運上，強化資安事件處理及維運之能量。

(3) 雲端資安攻防平台運作機制

為強化平台資安防護之能力，在架構規劃上導入不同的防護機制，如圖 9，對外防禦已針對常見的資安攻擊手法，例如：分散式阻斷服務攻擊、網站服務攻擊、系統及應用程式服務攻擊...等等，部署相對應的資安防護機制，內部防禦則採用 VLAN 切割搭配 ACL 存取控制進行嚴格的管控，並針對服務需求進行網段的劃分，以避免遭受非授權的存取或入侵。

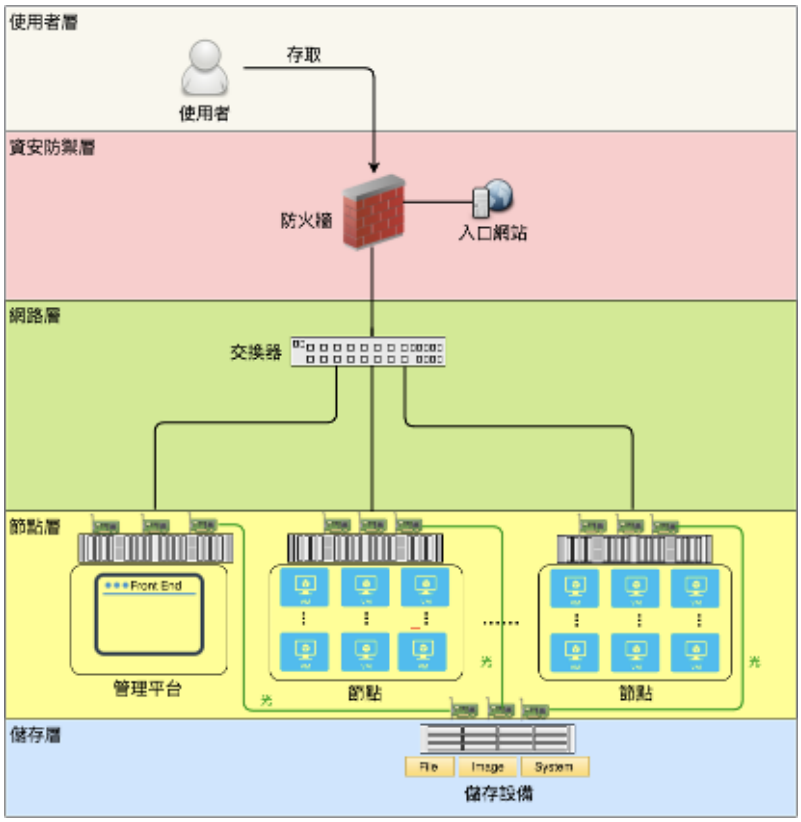

圖 11 平台簡易架構

另外，考量雲端多租戶環境的效能需求，平台在儲存架構上採用多種不同的機制，並運行於全高速的網路環境下，主要區分成系統環境及映像檔兩大區塊，前者為虛擬機器運行時所需的相關檔案，後者為部署虛擬機器所需的映像檔。系統環境部分採用分散式儲存的方式，透過多個運算節點的空間，進行檔案的儲存、切割及備援，可讓檔案讀取及寫入的速度更快。映像檔部份則是採用集中儲存的方式，藉由共享的方式進行檔案的存取，因此可以更容易做管理。

對於資安培訓及演練環境來說，獨立的隔離網路環境是非常重要的，

此平台架構設計方式與常見的公有雲服務不太一樣，因資安演練過程會需要部署存在系統漏洞的主機，如果這些機器直接公開放置於網路上，勢必會容易遭受到駭客的入侵，而變成惡意的中繼站導致發生資安事件。因此，在平台架構設計上需採用虛擬私有網路的方式，所有演練及培訓環境所需的機器，都必須部署於獨立的封閉環境內，使用者必須透過 VPN 連線的方式才能進行存取，且必須進行嚴格的網路連線控管，如此才可避免資安事件的發生。

雲端資安攻防平台經過多年的維運，陸續蒐集許多來自使用者的回饋意見，維運及開發團隊也持續進行功能改善，其中包括管理介面、權限控管、系統效能、操作流程...等等，舊版的 CDX1.0 已於 2019 年第 4 季正式下線，並正式升級為新版的 CDX2.0 系統。除了進行底層機器管理系統的升級之外，亦依據使用者回饋意見及團隊討論需求，進行新版網站整合介面的功能設計，可提供的服務功能如下：

帳號申請：提供線上申請表單，完成後自動開通 14 天試用帳號權限，正式帳號需要額外填寫表單進行申請。

公告管理：提供管理公告及發佈的功能，以及依據類型進行分類及呈現，亦可支援郵件寄送通知功能。

活動管理：提供管理活動上架及發佈的功能，可建立多個不同場次的活動，並結合報名系統進行人數統計。

群組管理：

提供群組帳號管理功能，可支援群組帳號增刪與異動、批次功能(匯入、刪除、配額)、助教權限指派、群組成員搜尋。

提供群組資源使用量統計資訊：CPU 使用量、記憶體使用量、已建立機器數量。

機器管理

一般機器：提供機器管理功能，可透過範本建置攻防所需之環境，並針對不同角色進行權限劃分，可支援功能為機器增刪、機器狀態操作(開機、關機、重啟、釋放資源)、延長關機時間、搜尋機器...等。為確保節點資源能夠有效地被利用，CDX2.0 改版後開始導入機器資源管控的機制，預設情況下每天均會釋放所有運行中機器的資源，但使用者可透過延長關機的功能，保留不需要被釋放資源的機器，最多可延

長時間為三天。

課程機器：提供課程機器管理功能，與一般機器不同的地方在於機器分組，課程機器會依據課程單元綁定的範本數量，建置相對應的機器組於系統上，同時亦支援指派不同網卡的功能，以及網路拓墣圖的呈現，可輔助課程學員理解網路狀況。

課程管理

課程及單元：提供課程及單元管理功能，採用階層式概念進行設計，分別為課程、主題及單元三種，課程為最外層的大框架，中間層則為主題的對應,最底層才是單元的綁定。現階段已可支援課程分享功能，課程教師可透過此功能與他人合作，共同推廣所屬之資安課程及教材，未來將規劃開放單元分享功能，可把不同學校設計的單元模組，綁定至同一門課程中，以增加其領域的多元性。

課程資源：提供課程資源檢視及瀏覽使用，可透過課程內的單元建立相關之環境，並搭配課程內提供的教材及影相進行學習，亦可參考授課時數當作時程上的規劃，以理論及實作的方式可大幅提升相關技術之能力。

系統管理：提供管理人員所需之功能，包括帳號管理、網路管理、範本管理、日誌管理四大項功能。

三、目前環境需求分析與未來環境預測說明

（一） 全球資訊安全推動現況

1. 以色列：透過軍中帶頭推動國家資安發展，以色列 8200 部隊是以色列國防軍中規模最大的獨立軍事單位,透過資訊化創新部隊進行嚴格培訓與研發。政府也投入 5 億美元進行強力推動以建立網路安全生態系統」,隨時注意與掌握網路安全與新興技術在產業與市場動態。
2. 韓國：韓國政府以預算無上限的方式進行資安推動，建構資安產業良性發展的架構及打造強化全球競爭力的生態體系。以「K-ICT Security 2020」規劃，設定 2020 年扶植資訊安全產業發展：(1)「透過強化資訊安全產業基礎去創造未來成長動力」、(2)「開發可取得市場先進者優勢的原始技術」,(3)「精銳資訊安全人才養成和資訊安全實踐文化建設」,以及(4)「提高網路資訊安全復原力所需資金的擴大」。
3. 日本：2018 年 7 月 27 日公布網路安全戰略，主要目的係持續實現「提昇

經濟社會活力與永續發展」、「實現國民安全且安心生活之社會」、「維持國際社會和平、安定與保障日本安全」三大目標。利用先進技術支持創新網路安全業務，制定網路安全措施指南，並對物聯網網路攻擊從不同角度進行劃分來採取措施，並透過國際合作與標準化來達到安心生活的社會。

4. 美國：由國土安全委員會批准於 2018 年通過「關鍵基礎設施資安防護法案」，在強化關鍵基礎設施系統抵禦網路攻擊能量與技術法案。幫助識別工業控制系統相關威脅，從而將國土安全部保護這些系統的工作任務法制化，並帶頭協調及處理跨關鍵基礎領域部門網路安全事件。2019 年通過「政府協助企業資安防護法案」，協助政府機關及私人企業避免網路攻擊，在這些組織遭到攻擊時也應協助緩解。

5. 德國：透過官方 BMBF 推動資訊科技安全研究計畫之一數位生活之資訊自主權與安全，計畫目標為致力於開發使用者導向之保護個人資料隱私與新興技術之安全解決方案。

6. 荷蘭：荷蘭擁有全歐洲最大的資安產業聚落，透過情報、教育、訓練及新創，建立國家安全、都市安全、資訊安全、刑事及關鍵基礎設施防護的五大領域之專業能量。

（二） 未來我國資訊安全發展趨勢

時代的變遷與科技進步，資訊科技與網路已成為各國關鍵基礎建設，關係國家競爭力根本和人民福祉。加上中美貿易戰影響全球經濟，工研院產科國際所指出，現在是發展「安全產業鏈」的重要契機，2019 年臺灣資安產業產值達新臺幣 437.3 億元，年增率 11.1%，預估 2020 年我國資安產值應可達成新台幣 550 億元的目標。

總統蔡英文上任後，即將「資安即國安」列為國家重大政策，全力填補我國在「資安機制」、「資安人才」、與「資安自主研發」的不足。因國內資安產業發展瓶頸主要在於市場規模太小，無法吸引專業人才投入，因此資安人員招募不易，資安廠商也難以在技術研發上深耕，試煉場域不足也無法提升服務品質問題，加上有越來越多的新型資安問題，如何防範並挑戰市場機會，需要有更多的學術研究預先投入，進行前瞻技術研究，並建置實戰淬鍊場域，透過產學合作提升我國資訊安全技術與人才能量，漸而帶動國內資安產業技術升級與生態系建立，確保我國智慧國家之資訊安全，提升我國資安能見度。

四、本計畫對社會經濟、產業技術、生活品質、環境永續、學術研究、人才培育等之影響說明

本計畫將整合產學研跨域軟硬體資安能量，發展對抗新型態攻擊之資安防禦技術，協助我國八大關鍵基礎設施，研發快速反應與防禦保護機制，提升產業資安防禦能量。建置資安攻防新興主題實測場域，促成資安攻防解決方案與新興智慧應用結合、發展跨域資安整體解決方案。本計畫對各層面的影響說明如下:

1. 產業技術面：研發尖端資安技術，針對 5G (B5G)、IoT 與 AI 等相關應用潛在威脅，研發先進資安技術與防護機制。
2. 人才培育面：進行前瞻關鍵資安技術學研成果落地沙崙資安基地，進行資安實務人才育成，培育產業所需之資安人才，並透過資安科技研究中心接軌國際資安能量。
3. 產業面：藉由前瞻關鍵資安技術或機制促成產學研鏈結，活躍學研能量，擴散資安技術研發成果，強化我國資安產業生態系。

參、計畫目標與執行方法

1. 目標說明

政府將「資安即國安」列為國家重大政策，「資安即國安 2.0 戰略」更著重提高人才培訓能量及開發資安創新技術。本計畫也因應越來越多的新型資安問題，鼓勵更多學術老師投入資訊安全領域，計畫目標為：

1. 軟硬結合、資安創新

針對關鍵基礎可能遭遇的資訊威脅，找出未來可能遭遇的資通訊威脅，開發相對應前瞻資安防護技術。

2. 資安資源共享與場域淬鍊

以資安科技研究中心為核心，透過專家會議研擬具突破性之尖端研究課題；並整合基礎研究資源，透過共享平台服務，於前期驗證環境淬鍊研發成果。

3. 國際接軌、共同合作

資安為當前國際性之重要研究、開發與產業議題，透過至國際先進資安研發單位進行移地研究，與共同研究或開發資安技術與機制，有利於提高我國在資安領域之國際地位與技術水平。

計畫全程總目標(end point)					
1. 強化未來新興科技資安防禦能量，確保智慧國家資訊安全。 2. 打造產官學交流合作平台，橋接未來科技研發與產業需求。 3. 提升國際能見度，建立國際資安研發領先地位。					
里程碑(milestone)					
年度	第一年 民 110 年	第二年 民 111 年	第三年 民 112 年	第四年 民 113 年	第四年 民 114 年 (8 月)
年度目標	1. 軟硬結合、資安創新 2. 資安場域、淬鍊技術 3. 國際接軌、共同合作	1. 軟硬結合、資安創新 2. 資安場域、淬鍊技術 3. 國際接軌、共同合作	1. 軟硬結合、資安創新 2. 資安資源共享與場域淬鍊 3. 國際接軌、共同合作	1. 軟硬結合、資安創新 2. 資安資源共享與場域淬鍊 3. 國際接軌、共同合作	1. 軟硬結合、資安創新 2. 資安資源共享與場域淬鍊 3. 國際接軌、共同合作
預期關鍵成果	1. 開發 10 項前瞻關鍵資安技術或機制，促成產學合作 15 件或技轉 3 件或總金額	1. 開發 10 項前瞻關鍵資安技術或機制，促成產學合作 15 件或技轉 3 件或總金額	1. 開發 15 項前瞻關鍵資安技術或機制，促成產學合作案 15 件或技轉 3 件或總金額	1. 開發 20 項前瞻關鍵資安技術或機制，促成產學合作案 15 件或技轉 3 件或總金額	1. 促成產學合作或技術移轉案 6 件或總金額達 300 萬以上。 2. 資安尖端研究中長期戰

	達 600 萬以上。 2. 完成 2 項產業場域研究與建置(Blue Team、Red Team Offense)，發展資安人才培訓情境，辦理新興科技資安攻防實務人才培訓 90 人次。 3. 培育高階資安技術研發人才 125 人、參與國際頂尖研討會發表論文 8 篇。	達 600 萬以上。 2. 完成 2 項產業場域研究與建置(IoT、Bank Hacking)，發展物聯網共同場域以及工業控制應用專屬場域等培訓情境，辦理新興科技資安攻防實務人才培訓 90 人次。 3. 培育高階資安技術研發人才 125 人、參與國際頂尖研討會發表論文 8 篇。	達 700 萬以上。 2. 資安尖端研究中長期戰略規劃報告 1 份，並促使 10 組研發團隊使用整合軟體資源服務。 3. 推動 1 場 100 人以上全國性雲端資安攻防競賽活動。 4. 培育高階資安技術研發人才 125 人、參與國際頂尖研討會發表論文 10 篇。 5. 2 次資安產學研高峰座談 6. 參與或主導大型跨國資安研究計畫 2 案	達 800 萬以上。 2. 資安尖端研究中長期戰略規劃報告 1 份，並促使 15 組研發團隊使用整合軟體資源服務。 3. 推動 1 場 100 人以上全國性雲端資安攻防競賽活動。 4. 培育高階資安技術研發人才 125 人、參與國際頂尖研討會發表論文 12 篇。 5. 2 次資安產學研高峰座談 6. 參與或主導大型跨國資安研究計畫 3 案	略規劃報告 1 份，並促使 15 組研發團隊使用整合軟體資源服務。 3. 推動 1 場 100 人以上全國性雲端資安攻防競賽活動。 4. 專利 5 件/全期程、國際間攻防平台發展趨勢與功能分析技術報告 4 份/全期程、先進國家移地研究 3 件/全期程或邀請國際頂尖資安專家來台演講 3 場/全期程
年度目標達成情形(重大效益)	1. 新增 64 項資安技術或機制研發，促成 13 件產學合作、3 件檢測與驗證服務與 1 件技術移轉，合計 17 件共 1,365 萬元。 2. 完成 2 項產業場域研究與建	1. 新增 52 項資安技術或機制研發，促成 26 件產學合作、1 件技術移轉，合計 27 件共 2,087.19 萬元。 2. 完成 2 項產業場域研究與建置 (IoT、Bank Hacking)，	1. 新增 252 項資安技術或機制研發，促成 47 件產學合作、3 件技術檢測服務，合計 50 件共 4,139 萬元。 2. 完成資安尖端研究戰略規劃年度報告英、美、	1. 至 113 年 4 月底，新增 173 項資安技術或機制研發，促成 8 件產學合作，合計 8 件共 562.8 萬元。 2. 至 113 年 4 月底，新增培育高階資安技術研發人	

	置 (Blue Team 、Red Team Offense)，發展資安人才培訓情境，並辦理新興科技資安攻防實務人才培訓227人次。 3. 新增培育高階資安技術研發人才300人，新增發表國際論文66件，其中國外重要期刊30件。	發展物聯網共同場域以及工業控制應用專屬場域等培訓情境，並辦理新興科技資安攻防實務人才培訓749人次。 3. 新增培育高階資安技術研發人才237人，新增發表國際論文98件，其中國外重要期刊共44件。	日、以色列國際政策與七大領域研究趨勢盤點，並提出短中長期策略，並促使11組研發團隊使用整合軟體資源服務。 3. 推動1場100人以上全國性雲端資安攻防競賽活動。 4. 新增培育高階資安技術研發人才341人，國際頂尖資安期刊/研討會發表論文新增發表國際論文56件，其中國外重要期刊共46件。 5. 舉辦2次資安產學研高峰座談。 6. 參與大型跨國資安研究計畫2案。	才75人，新增發表國際論文51件，其中國外重要期刊共28件。 3. 其餘113年關鍵成果持續規劃推動辦理中。	

2. 執行策略及方法

細部計畫名稱	執行策略說明(請依細部、子項計畫逐層說明)
前瞻資安技術研究 (Security in Air & Security on Chip)	(1)開發軟體資安技術(Security in Air) ● 研發成果擴散產業界，帶動國內資安產業發展 ● 建立資安技術自主創新，提高資安研發人才供給，帶動資安產業升級，推動資安產業聚落與生態系的形成與發展 (2)開發硬體資安晶片(Security on Chip) ● 透過 PUF 技術以加強晶片安全防護 ● 基於安全設計的 EDA 工具與環境應用 ● 旁通道攻擊的防禦機制 ● 應用國際開源的晶片安全框架技術
資安科技擴散及共享服務	(1)資安科技短中長期策略規劃 ● 透過資安科技研究中心專案執行辦公室進行效益分析與工作進度追蹤。 ● 提出具備國家資安戰略思惟的策略規劃。 (2)基礎資源整合與實證環境建構 ● 持續發展雲端資安攻防平台 (3)育才與國際合作鏈結 ● 培育資安實務人才 ● 接軌國際組織交流

3. 達成目標之限制、執行時可能遭遇之困難、瓶頸與解決的方式或對策

1. 資安專任人力招聘與續留困難，目前暫以研究生人力補足人力缺口。
2. 將來預計透過不同的人才培育模式建立專業人物、人才、人手，擴大到產業人才培訓等，逐步建立資安人才生態系。
3. 本計畫積極落實性別平等教育與性別平等教育白皮書之規劃，鼓勵學生適性揚才。

4. 與以前年度差異說明

年度 差異項目	112-113 年度	114 年度
資安技術研發及應用	112 年: 開發 15 項前瞻關鍵資安技術或機制，促成產學合作案 15 件或	促成產學合作或技術移轉案 6 件或總金額達 300 萬以上。

	技轉 3 件或總金額達 700 萬以上。 113 年: 開發 20 項前瞻關鍵資安技術或機制，促成產學合作案 15 件或技轉 3 件或總金額達 800 萬以上。	
國際接軌或合作	112 年: (1)辦理 2 次資安產學研高峰座談。 (2)參與或主導大型跨國資安研究計畫 2 案。 113 年: (1)辦理 2 次資安產學研高峰座談。 (2)參與或主導大型跨國資安研究計畫 3 案。	先進國家移地研究 3 件/全期程或邀請國際頂尖資安專家來台演講 3 場/全期程。
提升資安研究量能	112 年: 培育高階資安技術研發人才 125 人、參與國際頂尖研討會發表論文 12 篇。 113 年: 培育高階資安技術研發人才 125 人、參與國際頂尖研討會發表論文 12 篇。	專利 5 件/全期程、論文發表引用 50 人次/全期程、國際間攻防平台發展趨勢與功能分析技術報告 4 份/全期程。

5. 跨部會署合作說明

本計畫無。

6. 與本計畫相關之其他預算來源、經費及工作項目

本計畫無。

肆、前期重要效益成果說明

一、分年度重要執行成果

110 年度重要執行成果

(一) 新增64項資安技術或機制研發，促成13件產學合作、3件檢測與驗證服務與1件技術移轉，合計17件共1,365萬元。

(二) 完成2項產業場域研究與建置(Blue Team、Red Team Offense)，發展資安人才培訓情境，並辦理新興科技資安攻防實務人才培訓227人次。

(三) 新增培育高階資安技術研發人才300人，新增發表國際論文66件，其中國外重要期刊30件。

111 年度重要執行成果

(一)新增52項資安技術或機制研發，促成26件產學合作、1件技術移轉，合計27件共2,087.19萬元。

(二)完成 2 項產業場域研究與建置(IoT、Bank Hacking)，發展物聯網共同場域以及工業控制應用專屬場域等培訓情境，並辦理新興科技資安攻 防實務人才 培訓749人次。

(三)新增培育高階資安技術研發人才237人，新增發表國際論文98件，其中國外重要期刊共44件。

112 年度重要執行成果

(一)新增252項資安技術或機制研發，促成47件產學合作、3件技術檢測服務，合計50件共4,139萬元。

(二)完成資安尖端研究戰略規劃年度報告英、美、日、以色列國際政策與七大領域研究趨勢盤點，並提出短中長期策略，並促使11組研發團隊使用整合軟體資源服務。

(三)推動1場100人以上全國性雲端資安攻防競賽活動。

(四)新增培育高階資安技術研發人才341人，並以國際頂尖資安期刊/研討會發表論文為目標，積極提升資安學術成果質量，新增發表國際論文56件，其中國外重要期刊共46件。

(五)舉辦2次資安產學研高峰座談。

(六)參與大型跨國資安研究計畫2案。

113 年度重要執行成果

(一)至113年4月底，新增173項資安技術或機制研發，促成8件產學合作，合計8件共562.8萬元。

(二)至113年4月底，新增培育高階資安技術研發人才75人，並以國際頂尖資安期刊/研討會發表論文為目標，積極提升資安學術成果質量，新增發表國際論文51件，其中國外重要期刊共28件。

(三)其餘113年關鍵成果持續規劃推動辦理中。

二、里程碑達成情形

110 年至 112 年之里程碑皆已達成，113 年里程碑持續推動辦理中。

三、可量化經濟效益

截至 112 年底，累計促成 87 件產學合作、3 件檢測與驗證服務與 2 件技術移轉，合計 92 件合作案共 7,856 萬。113 年 4 月底新增促成 8 件產學合作，合計 8 件共 562.8 萬元。

四、不可量化經濟效益

(一) 本專案計畫以社會、產業與國家需求為導向(end-point)，規劃從上而下(top-down)的前瞻資安技術研究發展策略：針對軟、硬、韌體潛在資安威脅與產官學重要資安議題，觀察國內外資安技術發展趨勢，開發對應之創新前瞻資安主動式防禦技術，並期許能有效實現技術落地與提升產業應用價值。

(二) 透過模擬現實中企業常見使用之網路環境或系統服務架構開發新興科技擬真攻防場域，配合相關歷年曾發生過的資安風險與漏洞，用以建置發展擬真型的資安演練場域，以切合企業營運相關的實際環境，除了提供攻擊方（Red Team）在攻擊手法的演練與實證外，亦能提供防守方（Blue Team）實際測試防禦手法及檢視弱點修補的成效，能有效提升產業資安實務人才培育成效，下降人才培育成本。

伍、預期效益及效益評估方式規劃

1. 預期效益：

(1) 技術面：研發尖端資安技術，針對 5G(B5G)、IoT 與 AI 等相關應用潛在威脅，研發先進資安技術與防護機制。

(2) 人才面：進行前瞻關鍵資安技術學研成果落地沙崙資安基地，進行資安實務人才育成，培育產業所需之資安人才，並透過資安科技研究中心接軌國際資安能量。

(3) 產業面：藉由前瞻關鍵資安技術或機制促成產學研鏈結，活躍學研能量，擴散資安技術研發成果，強化我國資安產業生態系。

2. 效益評估方式規劃：

(1) 技術面：

(1.1) 因技術開發屬於前瞻研究範疇，採用專利申請數、專家學者引用研發成果、論文等方式進行評估。

(1.2) 由產學研專家委員依據本計畫之研發成果，評估是否為我國之關鍵資訊安全技術或防護機制。

(2) 人才面：

(2.1)由本計畫培育之博碩士生、博士後研究員及研究助理之人才數目，以及相關研究成果發表於資安領域國際期刊、研討會、邀至國際活動演講(如以色列資安週)或參加資安競賽名次進行評估。

(2.2)由本計畫所培訓之跨領域資安人才之數量以及參與資安競賽活動之人數，評估此計畫協助國內學界及業界培植資安人才。

(3) 產業面：

(3.1)透過產學合作件數、技術轉移件數、業者投入資金、投入人力進行評估。

(3.2)由團隊與業界合作廠商數目、合作方式、實證場域攻防演練參加人數、資安技術論壇場數，評估是否達成產業效益目標。

(3.3)將雲端資安攻防平台導入資安業者產品，了解企業使用率與下載數，評估產業在功能與安全性驗證。

陸、自我挑戰目標

114 年度

114 年度係本計畫最後一期計畫，擬於 8 個月內就國際交流部分，挑戰與先進國家合作，強化移地研究或邀請國際頂尖資安專家來台之工作，並與國外學者共同發表論文 6 篇，提升臺灣資安領域能見度。

(請附 112 年度及 113 年度挑戰目標及達成情形)

112 年度

1. 針對未來新型態攻擊之資安防禦技術與資訊科技的應用情境，進行下一世代資安關鍵技術或機制的研發，挑戰開發 15 項相關之前瞻關鍵資安技術與機制。

   達成情形：已新增 252 項資安技術或機制研發。

2. 經由研發技術及場域實戰淬鍊過程，培育資安技術研發人才，挑戰培育高階資安技術研發人才達 150 人。

   達成情形：新增培育高階資安技術研發人才 341 人。

3. 促進產學合作及技術移轉，以擴散資安專案的研發成果與能量，帶動國內資安產業技術升級與研究生態系的建立，挑戰促成產學合作總金額達 1000 萬以上。

   達成情形：促成 26 件產學合作、1 件技術移轉，合計 27 件共 2,087.19 萬元。

4. 透過移地研究、參與國際會議與國際學術交流活動，鏈結與強化國際合作關係，以利提升我國資安技術水平，挑戰出席或參與國際研討會達 15 場。

   達成情形：出席或參與國際研討會超過 15 場，並於國際研討會新增發表國際論文 56 件。

5. 融合國內產學研需求，並鏈結國際，提出具備資安尖端研究戰略思惟的策略規劃。

   達成情形：完成資安尖端研究戰略規劃年度報告英、美、日、以色列國際政策與七大領域研究趨勢盤點，並提出短中長期策略。

6. 對焦全球資安議題，策略引導研究團隊進行國際合作，挑戰參與或主導大型跨國資安研究計畫 2 案。

   達成情形：參與大型跨國資安研究計畫 2 案。

113 年度

1. 針對未來新型態攻擊之資安防禦技術與資訊科技的應用情境，進行下一世代資安關鍵技術或機制的研發，挑戰開發 20 項相關之前瞻關鍵資安技術與機制。

   達成情形：至 113 年 4 月底，新增 173 項資安技術或機制研發。

2. 經由研發技術及場域實戰淬鍊過程，培育資安技術研發人才，挑戰培育高階資安技術研發人才達 150 人。

   達成情形：至 113 年 4 月底，新增培育高階資安技術研發人才 75 人，持續挑戰目標中。

3. 促進產學合作及技術移轉，以擴散資安專案的研發成果與能量，帶動國內資安產業技術升級與研究生態系的建立，挑戰促成產學合作總金額達 1200 萬以上。

   達成情形：促成 8 件產學合作，合計 8 件共 562.8 萬元，持續挑戰目標中。

4. 透過移地研究、參與國際會議與國際學術交流活動，鏈結與強化國際合作關係，以利提升我國資安技術水平，挑戰出席或參與國際研討會達 15 場。

   達成情形：持續挑戰目標中。

5. 融合國內產學研需求，並鏈結國際，提出具備資安尖端研究戰略思惟的策略規劃。

   達成情形：持續挑戰目標中。

6. 對焦全球資安議題，策略引導研究團隊進行國際合作，挑戰參與或主導大型跨國資安研究計畫 3 案。

   達成情形：持續挑戰目標中。

柒、經費需求/經費分攤/槓桿外部資源

經費需求表(B005)

單位：千元

細部計畫名稱	計畫屬性	114 年度(8 月)		
		小計	經常支出	資本支出
細部計畫 1: 前瞻資安技術研究 (Security in Air & Security on Chip)	基礎研究	46,200	46,200	0
細部計畫 2:資安科技擴散及共享服務	基礎研究	28,800	28,500	300

A. 組織維運/類業務：常態性支持與維運法人組織運作，或為支持科研發展衍生之常規性業務或研究等計畫。

B. 資通訊建設：以資通訊設備建置為計畫核心，目的在於推動資訊化社會之建設，建構完善基礎環境，規劃資訊通信關鍵應用，以帶動資訊國力提升。

C. 人才培育：計畫主軸係以人才培育為核心策略，以人力資本的投入帶動基礎研究、產業發展或轉型及公共民生之發展。

D. 基礎研究：非以專門或特定應用/使用為目的，成果不特別強調與產業的連結性；或為目前已知或未來預期面臨之問題，但尚缺乏廣泛知識基礎而進行之研究。本屬性涵蓋基礎研究核心設施。

E. 產業技術研發：進行與產業連結性高之相關技術研究與開發。

F. 產業服務與應用：將科技研究與技術應用於產業，進而推動產業發展，包括技術及產品應用或產業輔導等。

G. 環境永續與社會發展：具永續性或有助於民生及公共福祉之公共資源、公共服務、科技政策等，於短、中、長期可促進各類人民福祉之提升、環境之保全與安全之促進。

114 年度經費需求表

經費需求說明

一、經費計算基準：如人事費以各級人力人數、薪資估算；儀器設備費以單價及數量估算總價等。

二、經費列於其他經常門支出或其他資本門支出者，請具體述明採購項目、單價、數量及用途，以利審查。

三、經費需求較上一年度預算有差異者，請填列經費增減說明。

四、編列儀器設備費者，應說明所建置之基礎設施或採購之儀器設備，與政府推動政策之配合情形(如自研自製，設備國產化等)。

五、請說明如何槓桿外部資源請說明如何槓桿外部資源，例如促進民間投入，或其他如公共建設、重要社會發展計畫等。

114 年度經費需求表

單位：千元

計畫名稱	細部計畫重點描述	預期關鍵成果	114 年度						
			小計	經常支出			資本支出		
				人事費	材料費	其他費用	土地建築	儀器設備	其他費用
一、細部計畫 1 前瞻資安技術研究(Security in Air & Security on Chip)	(1) 開發軟體資安技術(Security in Air) (2) 開發硬體資安晶片(Security on Chip)	1. 促成產學合作或技術移轉案 6 件或總金額達 300 萬以上。 2. 專利 5 件/全期程、論文發表引用 50 人次 / 全期程、國際間攻防平台發展趨勢與功能分析技術報告 4 份/全期程、先進國家移地研究 3 件/全期程或邀請國際頂尖資安	46,200	34,650	5,775	5,775	0	0	0

		專家來台演講3場/全期程。							
二、**細部計畫2** 資安科技擴散及共享服務	(1) 資安科技短中長期策略規劃 (2) 基礎資源整合與實證環境建構 (3) 育才與國際合作鏈結	1. 完成資安尖端研究中長期戰略規劃報告1份，並促使15組研發團隊使用整合軟體資源服務。 2. 推動1場100人以上全國性雲端資安攻防競賽活動。	28,800	18,000	5,400	5,100	0	0	300

經費分攤表(B008)

114 年度

跨部會 主提/合提機關 (含單位)	細部計畫名稱	負責內容	預期關鍵成果	經費額度
經費合計				

本計畫無。

捌、儀器設備需求

(如單價 1000 萬以上儀器設備需俟受補助對象申請通過才採購而暫無法詳列者，嗣後應依規定另送科技部審查)

申購單價新臺幣 1000 萬元以上科學儀器送審彙總表(B006)

申請機關：

(單位：新臺幣千元)

年度	編號	儀器名稱	使用單位	數量	單價	總價	優先順序		
							1	2	3
114	1								
	2								
	3								
	4								
	5								
	6								
總計									

本計畫無。

填表說明：

1. 申購單價新臺幣 1000 萬元以上科學儀器設備者應填列本表。
2. 本表中儀器名稱以中文為主，英文為輔。
3. 本表中之優先次序欄內，請確實按各項儀器採購之輕重緩急區分為第一、二、三優先。
   (1) 「第一優先」係指為順利執行本計畫，建議預算有必要充分支援之儀器項目。
   (2) 「第二優先」係指當本計畫預算刪減逾 10%時，得優先減列之儀器項目。
   (3) 「第三優先」係指當本計畫預算刪減逾 5%時，得優先減列之儀器項目。

（主管機關名稱）

申購單價新臺幣 1000 萬元以上科學儀器送審表(B007)

中華民國 xxx 年度

(參考系統格式填寫)

申請機關(構)					
使用部門					
中文儀器名稱					
英文儀器名稱					
數量		預估單價(千元)		總價(千元)	
購置經費來源	□申請機構作業基金(基金名稱：　　) □行政院國家科學技術發展基金(計畫名稱：　　) □政府科技預算(政府機關名稱：　　) □前瞻基礎建設特別預算(計畫名稱：　　) □其他(說明：　　)				
期望廠牌					
型式					
製造商國別					

一、儀器需求說明

1.需求本儀器之經常性作業名稱：

2.儀器類別：(醫療診斷用儀器限醫療機構得勾選；公務用儀器係指執行法定職掌業務所需儀器，限政府機關得勾選)

□醫療診斷用儀器　□政府機關公務用儀器　□教學或研究用儀器

3.儀器用途：

4.購置必要性說明：(請詳述購置需求，以免因無法檢視儀器必要性而導致負面審查結果)

二、目前同類儀器(醫療診斷及公務用儀器專用)

1.本儀器是

□新購(申請機構無同類儀器)

□增購(申請機構雖有同類儀器，但已不符或不敷使用)

□汰購(汰舊換新)

2.若為增(汰)購，請將申請機構目前使用之同類儀器名稱、廠牌、型式、購買年份及使用狀況詳列於下：

儀器名稱	型式	廠牌	年份	數量	使用現況

二、目前同類儀器(教學或研究用儀器儀器專用)

1.本儀器是

□新購(申請機構所在區域無同類儀器)

□增購(申請機構所在區域雖有同類儀器，但已不符或不敷使用)

□汰購(汰舊換新)

2.若為增(汰)購，請將申請機構所在區域目前使用之同類儀器名稱、廠牌、型式、購買年份(未知可免填)及使用狀況詳列於下：

儀器名稱	儀器所屬機構名稱	型式	廠牌	年份	數量	使用現況

註：1000 萬元以上科學儀器請優先考量共用現有設備，並可至「貴重儀器開放共同管理平台」查詢同類儀器；如經查詢現有設備有規格不符需求、開放時段不敷使用、至設備所在位置交通成本偏高等情形，再考量購置之必要性。

三、儀器使用計畫

1.請詳述本儀器購買後 5 年內之使用規劃及其預期使用效益。(非醫療診斷用儀器請務必填寫近 5 年可能進行之研究項目或計畫)

(1)使用規劃：

(2)預期使用效益：

2.維護規劃：(請填寫儀器維護方式、預估維護費及經費來源等)

3.請詳述本儀器購買後 5 年內之擴充規劃(含配備升級等)，如儀器為整個系統之一部分，則請填寫系統擴充規劃。

(1)儀器是否為整個系統之一部分？

□否

□是，系統名稱：_____

(2)擴充規劃：

4.儀器使用時數規劃

	1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月	總時數
可使用時數													
自用時數													
對外開放時數													

(1)可使用時數估算說明：

(2)自用時數估算說明：

(3)對外開放時數及對象預估分析：

四、儀器對外開放計畫

□儀器對外開放，開放規劃如下：(請就管理方式、服務項目、收費標準等詳細說明，開放方式可能包含提供使用者自行檢測及分析、接受委託檢測但由使用者自行分析、接受委託檢測及分析等)

□本儀器為整個系統之一部分，系統已對外開放，開放方式如下：

□不對外開放，理由為：(除醫療診斷用及政府機關公務用儀器外，教學或研究用儀器原則對外開放，如未開放須詳述具體理由)

□醫療診斷用儀器，為醫療機構執行醫療業務專用。

□儀器為政府機關執行法定職掌業務所需，以公務優先。

□教學或研究用儀器，說明：_____

五、儀器規格

請詳述本儀器之功能及規格，諸如靈敏度、精確度及重要特性、重要附件與配合設施，並請附送估價單及規格說明書。

1.詳述功能及規格：

2.估價單(除有特殊原因，原則檢附 3 家估價單)

□僅附送_____家估價單，原因為：_____

六、廠牌選擇與評估

1.如擬購他國產品，請說明其理由。

□國產品

□他國產品，原因為：_____

2.比較可能供應廠牌之型式、性能、購置價格、維護保固、售後服務等優缺點，以及對本單位之適合性。

	廠牌(一)	廠牌(二)	廠牌(三)	…
比較項目(一)				
比較項目(二)				
比較項目(三)				
比較項目(四)				

七、人員配備與訓練

1.請詳列本儀器購進後使用操作人員簡歷(如有待聘人力，請於姓名欄位註明待聘，餘欄位填列待聘人力之學經歷要求)

姓名	性別	年齡	職稱	學歷	專長	有否受過相關訓練 （請列名稱）

2.使用操作人員進用、調配、訓練規劃(待聘人力須述明進用規劃)

□無

□有，規劃如下：_____

八、儀器置放環境

1.請描述本儀器預定放置場所之環境條件。(非必要條件，請填無)

空間大小	平方公尺	相對濕度	%～ %
電壓幅度	伏特～ 伏特	除濕設備	
不斷電裝置		防塵裝置	
溫度	℃～ ℃	輻射防護	
其他			

2.環境改善規劃

□無，預定放置場所已符合儀器所需環境條件。

□有，環境改善規劃及經費來源如下：

(1)擬改善項目包含：_____。

(2)環境改善措施所需經費計_____千元。

(3)環境改善措施經費來源：

□尚待籌措改善經費。

□改善經費已納入本申請案預估總價中。

□改善經費已納入____年度_____預算編列。

九、優先順序

請列出本儀器在機關提出擬購儀器清單中之優先購買順序，並說明其理由。

□第一優先：為順利執行本計畫，建議預算充分支援之儀器項目。

□第二優先：當本計畫預算刪減逾 10%時，得優先減列之儀器項目。

□第三優先：當本計畫預算刪減逾 5%時，得優先減列之儀器項目。

理由說明：_____

本計畫無。

玖、就涉及公共政策事項，是否適時納入民眾參與機制之說明

本計畫無此事項。

拾、附錄

一、政府科技發展計畫自評結果(A007)

(一)計畫名稱：臺灣資安卓越深耕-學術型資安研究(5/5)
審議編號：114-1901-11-20-01
計畫類別：前瞻基礎建設計畫

(二)自評委員：林祝興、廖宜恩

日期：113 年 5 月 27 日

(三)審查意見及回復：
(應依據計畫可行性、過去績效、執行優先性、預算額度等，進行評估及建議，自評形式及次數請自行斟酌)

序號	審查意見	回復說明
1	本計畫依循我國資安戰略，透過資安技術研發與機制設計，並培育資安研發人才，期能建立我國「資安自主研發」之厚實基礎。並且以計畫目標、預期關鍵成果(OKR)及與部會科技施政目標之關聯、主要績效指標(KPI)呈現計畫內容，敘述清楚明瞭。	感謝委員的肯定。
2	本計畫之全程總目標為：(1)強化未來新興科技資安防禦能量,確保智慧國家資訊安全。(2)打造產官學交流合作平台，橋接未來科技研發與產業需求。(3)提升國際能見度，建立國際資安研發領先地位。本計畫目標明確可行。	感謝委員的肯定。
3	分項計畫一包含：(1)開發軟體資安技術、(2)開發硬體資安晶片。並擬定相關推動策略強化我國前瞻軟硬體資安研究與發展。二大面向條列敘述清楚，具體可行。	感謝委員的肯定。

4	分項計畫二包含：(1)資安科技短中長期策略規劃、(2)基礎資源整合與實證環境建構、(3)育才與國際合作鏈結。三大面向分析明瞭，亦具高可行性。	感謝委員的肯定。
5	本計畫之前三年期(110~112)重要效益成果在：資安技術或機制研發、產學合作、技術檢測服務、技術轉移等方面，成果績效均逐年成長。例如 112 年度即有：新增 252 項資安技術或機制研發，促成 47 件產學合作、3 件技術檢測服務，合計 50 件共 4,139 萬元。前三年重要成果均有良好之績效。	感謝委員的肯定。
6	依據前期主要績效的表現估算，113 年度預期關鍵成果：(1)開發 20 項前瞻關鍵資安技術或機制，促成產學合作案 15 件或技轉 3 件或總金額達 800 萬以上。以上此兩項 KPI 皆似宜再提升量能，增加數量或金額。	感謝委員的建議，有關研究團隊開發資安技術或機制及產學合作及技轉成果 113 年度皆有持續增加中，至 113 年 4 月底，已新增 173 項資安技術或機制研發，促成 8 件產學合作，合計 8 件共 562.8 萬元，目前進度應有望於 113 年底結束時，再增加產出績效之數量或金額，提升本計畫量能。
7	依據前期主要績效的表現估算，113 年度預期關鍵成果：(4)培育高階資安技術研發人才 125 人。在人才培育、資安科技擴散、共享服務方面似宜可再提升績效，再增加量能。	感謝委員的建議，有關在人才培育、資安科技擴散、共享服務方面，本計畫將持續以雲端資安攻防平臺(CDX)，提供學研團隊研發及育才使用，並訂定促使研發團隊使用整合軟體資源服務，推動 1 場百人以上之全國性雲端資安攻防競賽活動，113 年度尚在推動辦理中，將依委員建議朝增加產出績效努力，以提升本計畫量能。

8	依據前期主要績效的表現估算，113 年度預期關鍵成果：(4)參與國際頂尖研討會發表論文 12 篇。國際頂尖研討會、國外重要期刊發表論文等，宜再增加量能。	感謝委員的建議，本計畫因嚴格定義頂尖研討會為 Google H5 index 排名前五、頂尖期刊為 JCR 或 JIF 排名前五，目標在於督促研究團隊確實攻頂，進行質化提升，爰 113 年度訂定參與國際頂尖研討會發表論文 12 篇，惟 114 年度為本計畫之最後一年，爰指標規劃上未以增加發表論文篇數為標準，而是以發表論文之引用人次為主，以呈現本計畫學術攻頂全程執行成果。
9	在計畫書中，page 45，「3.達成目標之限制、執行時可能遭遇之困難、瓶頸與解決的方式或對策。」本節列舉三項，然皆是針對資安專任人力招聘與續留困難之問題，也僅作簡略敘述。似宜增加說明其他相關可能遭遇之問題。以及針對人才招募及留任之解決方案是否有更具體可行方案或對策？	謝謝委員的指正，資安專任人力招聘與續留困難仍為最可能遭遇困難之問題，主要原因在於目前產業薪資水準明顯高於國科會聘用標準，本計畫執行期間內僅能暫以使用兼任人力取代，更積極之方案仍需待逐年擴充資安師資，加大人才培育量能。
10	在計畫書中，page 46，「提升資安研究量能」，在培育高階資安技術研發人才、參與國際頂尖研討會發表論文方面。113 年度之預期績效似乎可以比 112 年度較為成長。	感謝委員的建議，自 112 年度起本計畫針對高階資安技術研發人才限縮為統計碩士班以上專兼任助理，在國際頂尖研討會也嚴格定義為 Google H5 index 排名前五之研討會，以確保計畫在質化效益的提升，爰 113 年度之預期量化績效仍維持 112 年度相同之數字。
11	近年來，有鑑於我國遭受到非常嚴厲的假訊息、社交媒體詐騙、認知戰等侵害，造成財物損失，破壞公眾信任、影響政府施政甚鉅。本計畫是否有機會可以思考融入一些對抗這些攻擊	感謝委員的建議，目前本計畫聚焦七大前瞻資安關鍵研究主題：晶片安全、後量子密碼、衛星安全防護、零信任架構、人工智慧資安、韌性網路、下世代行動網路安全。有關假訊息、社交

	之相關研究議題、或推廣宣導媒體識讀機制，例如：假訊息、可疑帳號偵測、社交媒體詐騙預警、認知戰提防等等，鼓勵更多研究資源及人力投入，相信對民生福祉必有相當助益。	媒體詐騙與認知戰加入研究主題之可能性將於後續推動時評估納入。
12	本計畫為「臺灣資安卓越深耕-學術型資安研究」，110-112 年的 KPI 量化成果佳，但建議能增加一些質化成果的說明，以展現本學術資安卓越計畫的特色。	感謝委員的建議。有關質化成果本計畫自 112 年度起係透過嚴格定義頂尖研討會為 Google H5 index 排名前五、頂尖期刊為 JCR 或 JIF 排名前五，目標在於督促研究團隊確實攻頂，而非僅增加論文發表數量，已於調整前期重要效益文字說明內容。(詳如第 47 頁)
13	本計畫自 112 年起於國科會成立台灣資安科技研究中心(Taiwan Academic Cybersecurity Center, TACC)推動辦公室，以整合資安學術成果，聚焦關鍵議題研究，促進國際拔尖，培育資安學術研究人才。這是很好的作法，讓台灣有國家級的學術資安研究中心，有助於和國際資安研究機構進行合作與交流。	感謝委員的肯定。
14	TACC 聚焦七大前瞻資安關鍵研究主題：晶片安全、後量子密碼、衛星安全防護、零信任架構、人工智慧資安、韌性網路、下世代行動網路安全。這些主題符合國際資安研發趨勢。	感謝委員的肯定。
15	112(113)年度里程碑有「國際頂尖研討會發表論文 8(10)篇」，建議修改為國際頂尖資安期刊/研討會發表論文。	感謝委員的建議，112 年度里程碑已修正為「國際頂尖資安期刊/研討會發表論文 10 篇」，113 年度里程碑已修正為「國

		際頂尖資安期刊/研討會發表論文 12 篇」。(詳如第 17 頁)。
16	113 年度已和數個國際資安機構如日本 NICT 進行合作，建議 114 年度自我挑戰目標的國際合作部分能有和國際學者共同發表論文的成果。	感謝委員的建議，114 年度已增加「與國外學者共同發表論文 6 篇」的自我挑戰目標。(詳如第 50 頁)。

二、中程個案計畫自評檢核表

檢視項目	內 容 重 點 (內容是否依下列原則撰擬)	主辦機關		主管機關		備註
		是	否	是	否	
1、計畫書格式	(1)計畫內容應包括項目是否均已填列(「行政院所屬各機關中長程個案計畫編審要點」（以下簡稱編審要點）第 5 點、第 10 點)	v		v		
	(2)延續性計畫是否辦理前期計畫執行成效評估，並提出總結評估報告(編審要點第 5 點、第 13 點)	v		v		本計畫皆有定期辦理計畫執行成效評估。
	(3)是否本於提高自償之精神提具相關財務策略規劃檢核表？並依據各類審查作業規定提具相關書件		v		v	本計畫無涉財物自償，爰無提供財務策略規劃檢核表。
2、民間參與可行性評估	(1)是否評估民間參與之可行性，並撰擬評估說明(編審要點第 4 點）		v		v	本計畫內容無涉。
	(2)是否填寫「促參預評估檢核表」評估（依「公共建設促參預評估機制」)		v		v	本計畫內容無涉。
3、經濟及財務效益評估	(1)是否研提選擇及替代方案之成本效益分析報告(「預算法」第 34 條)		v		v	本計畫內容無涉。
	(2)是否研提完整財務計畫		v		v	
4、財源籌措及資金運用	(1)經費需求合理性(經費估算依據如單價、數量等計算內容)	v		v		詳見本計畫經費估算內容。
	(2)資金籌措：本於提高自償之精神，將影響區域進行整合規劃，並將外部效益內部化		v		v	本計畫內容無涉。
	(3)經費負擔原則： a.中央主辦計畫：中央主管相關法令規定 b.補助型計畫：中央對直轄市及縣(市)政府補助辦法、本於提高自償之精神所擬訂各類審查及補助規定	v		v		本計畫為中央主辦計畫，依中央主管相關法令規定辦理。
	(4)年度預算之安排及能量估算：所需經費能否於中程歲出概算額度內容納加以檢討，如無法納編者，應檢討調減一定比率之舊有經費支應；如仍有不敷，須檢附以前年度預算執行、檢討不經濟支出及自行檢討調整結果等經費審查之相關文件	v		v		本計畫年度預算之安排及能量皆有檢討機制。
	(5)經資比 1:2(「政府公共建設計畫先期作業實施要點」第 2 點）		v		v	本計畫內容無涉。
	(6)屬具自償性者，是否透過基金協助資金調度		v		v	本計畫內容無涉。
5、人力運用	(1)能否運用現有人力辦理	v		v		
	(2)擬請增人力者，是否檢附下列資料： a.現有人力運用情形 b.計畫結束後，請增人力之處理原則 c.請增人力之類別及進用方式 d.請增人力之經費來源		v		v	本計畫內容無涉。
6、跨機關協商	(1)涉及跨部會或地方權責及財務分攤，是否進行跨機關協商		v		v	本計畫內容無涉。
	(2)是否檢附相關協商文書資料		v		v	本計畫內容無涉。
7、土地取得	(1)能否優先使用公有閒置土地房舍		v		v	本計畫內容無涉。
	(2)屬補助型計畫，補助方式是否符合規定(中央對直轄市及縣(市)政府補助辦法第 10 條)		v		v	本計畫內容無涉。
	(3)計畫中是否涉及徵收或區段徵收特定農業區之農牧用地		v		v	本計畫內容無涉。

檢視項目	內 容 重 點 (內容是否依下列原則撰擬)	主辦機關		主管機關		備註
		是	否	是	否	
	(4)是否符合土地徵收條例第 3 條之 1 及土地徵收條例施行細則第 2 條之 1 規定		v		v	本計畫內容無涉。
	(5)若涉及原住民族保留地開發利用者，是否依原住民族基本法第 21 條規定辦理		v		v	本計畫內容無涉。
8、風險管理	是否對計畫內容進行風險管理	v		v		詳見本計畫風險管理評估檢視表。
9、性別影響評估	是否填具性別影響評估檢視表	v		v		詳見本計畫性別影響評估檢視表。
10、環境影響分析(環境政策評估)	是否須辦理環境影響評估		v		v	本計畫內容無涉。
11、淨零轉型通案評估	(1)是否以二氧化碳之減量為節能減碳指標，並設定減量目標		v		v	本計畫內容無涉。
	(2)是否規劃採用綠建築或其他節能減碳措施		v		v	本計畫內容無涉。
	(3)是否強化因應氣候變遷之調適能力，並納入淨零排放及永續發展概念，優先選列臺灣 2050 淨零排放路徑、淨零科技方案及淨零轉型十二項關鍵戰略、臺灣永續發展目標及節能相關指標		v		v	本計畫內容無涉。
	(4)是否屬臺灣 2050 淨零排放路徑、淨零科技方案及淨零轉型十二項關鍵戰略相關子計畫		v		v	本計畫內容無涉。
	(5)屬臺灣 2050 淨零排放路徑、淨零科技方案及淨零轉型十二項關鍵戰略之相關子計畫者，是否覈實填報附表三、中長程個案計畫淨零轉型通案自評檢核表，並檢附相關說明文件		v		v	本計畫內容無涉。
12、涉及空間規劃者	是否檢附計畫範圍具座標之向量圖檔		v		v	本計畫內容無涉。
13、涉及政府辦公廳舍興建購置者	是否納入積極活化閒置資產及引進民間資源共同開發之理念		v		v	本計畫內容無涉。
14、落實公共工程或房屋建築全生命週期各階段建造標準	是否瞭解計畫目標，審酌其工程定位及功能，對應提出妥適之建造標準，並於公共工程或房屋建築全生命週期各階段，均依所設定之建造標準落實執行		v		v	本計畫內容無涉。
15、公共工程節能減碳及生態檢核	(1)是否依行政院公共工程委員會(下稱工程會)函頒之「公共工程節能減碳檢核注意事項」辦理		v		v	本計畫內容無涉。
	(2)是否依工程會函頒之「公共工程生態檢核注意事項」辦理		v		v	本計畫內容無涉。
16、無障礙及通用設計影響評估	是否考量無障礙環境，參考建築及活動空間相關規範辦理		v		v	本計畫內容無涉。
17、高齡社會影響評估	是否考量高齡者友善措施，參考 WHO「高齡友善城市指南」相關規定辦理		v		v	本計畫內容無涉。
18、營(維)運管理計畫	是否具務實及合理性(或能否落實營運或維運)	v		v		
19、房屋建築朝近零碳建築方向規劃	是否已依工程會「公共工程節能減碳檢核注意事項」及內政部建築研究所「綠建築評估手冊」之綠建築標章及建築能效等級辦理		v		v	本計畫內容無涉。
20、地層下陷影響評估	屬重大開發建設計畫者，是否依「機關重大開發建設計畫提報經濟部地層下陷防治推動委員會作業須知」辦理		v		v	本計畫內容無涉。
21、資通安全防護規劃	資訊系統是否辦理資通安全防護規劃		v		v	本計畫內容無涉。

主辦機關核章：承辦人 科員李丹容　單位主管 副處長王詔民　首長 主任委員吳誠文(乙)

主管部會核章：研考主管 處長彭麗春　會計主管 處長廖玉燕　首長 主任委員吳誠文(乙)

三、性別影響評估檢視表

中長程個案計畫性別影響評估檢視表【一般表】

【第一部分】：本部分由機關人員填寫

【填表說明】各機關使用本表之方法與時機如下：

一、計畫研擬階段

（一）請於研擬初期即閱讀並掌握表中所有評估項目；並就計畫方向或構想徵詢作業說明第三點所稱之性別諮詢員（至少 1 人），或提報各部會性別平等專案小組，收集性別平等觀點之意見。

（二）請運用本表所列之評估項目，將性別觀點融入計畫書草案：

1. 將性別目標、績效指標、衡量標準及目標值納入計畫書草案之計畫目標章節。
2. 將達成性別目標之主要執行策略納入計畫書草案之適當章節。

二、計畫研擬完成

（一）請填寫完成【第一部分－機關自評】之「壹、看見性別」及「貳、回應性別落差與需求」後，併同計畫書草案送請性別平等專家學者填寫【第二部分－程序參與】，宜至少預留 1 週給專家學者（以下稱為程序參與者）填寫。

（二）請參酌程序參與者之意見，修正計畫書草案與表格內容，並填寫【第一部分－機關自評】之「參、評估結果」後通知程序參與者審閱。

三、計畫審議階段：請參酌行政院性別平等處或性別平等專家學者意見，修正計畫書草案及表格內容。

四、計畫執行階段：請將性別目標之績效指標納入年度個案計畫管制並進行評核；如於實際執行時遇性別相關問題，得視需要將計畫提報至性別平等專案小組進行諮詢討論，以協助解決所遇困難。

註：本表各欄位除評估計畫對於不同性別之影響外，亦請關照對不同性傾向、性別特質或性別認同者之影響。

計畫名稱：			
主管機關 （請填列中央二級主管機關）	國科會	**主辦機關（單位）** （請填列擬案機關／單位）	前瞻處

1. **看見性別：**檢視本計畫與性別平等相關法規、政策之相關性，並運用性別統計及性別分析，「看見」本計畫之性別議題。

評估項目	評估結果
1-1【請說明本計畫與性別平等相關法規、政策之相關性】	本計畫執行內容以技術研發及人才培育為主，並在計畫諮詢規

性別平等相關法規與政策包含憲法、法律、性別平等政策綱領及消除對婦女一切形式歧視公約（CEDAW）可參考行政院性別平等會網站（https://gec.ey.gov.tw）。	劃會議中，安排女性專家學者參與，與性別平等政策綱領所強調消除性別隔離及營造性別友善工作環境、降低決策參與上的性別隔閡等重要議題相關。
評估項目	**評估結果**
1-2【請蒐集與本計畫相關之性別統計及性別分析（含前期或相關計畫之執行結果），並分析性別落差情形及原因】 請依下列說明填寫評估結果： a.歡迎查閱行政院性別平等處建置之「性別平等研究文獻資源網」 (https://www.gender.ey.gov.tw/research/)、「重要性別統計資料庫」(https://www.gender.ey.gov.tw/gecdb/)（含性別分析專區）、各部會性別統計專區、我國婦女人權指標及「行政院性別平等會─性別分析」(https://gec.ey.gov.tw)。 b.性別統計及性別分析資料蒐集範圍應包含下列 3 類群體： ①**政策規劃者**（例如:機關研擬與決策人員；外部諮詢人員）。 ②**服務提供者**（例如:機關執行人員、委外廠商人力）。 ③**受益者**（或使用者）。 c.前項之性別統計與性別分析應盡量顧及不同性別、性傾向、性別特質及性別認同者，探究其處境或需求是否存在差異，及造成差異之原因；並宜與年齡、族群、地區、障礙情形等面向進行交叉分析（例如：高齡身障女性、偏遠地區新住民女性），探究在各因素交織影響下，是否加劇其處境之不利，並分析處境不利群體之需求。前述經分析所發現之處境不利群體及其需求與原因，應於後續【1-3 找出本計畫之性別議題】，及【貳、回應性別落差與需求】等項目進行評估說明。 d.未有相關性別統計及性別分析資料時，請將「強化與本計畫相關的性別統計與性別分析」列入本計畫之性別目標（如 2-1 之ｆ）。	1. 本專案屬國防資安領域，該領域學者群體於科技領域學者群體中偏少數，又該領域諮詢專家更為稀少，全台灣長年深耕於資訊安全領域之學者約為 40 至 50 位。 2. 本計畫在先期規劃諮詢專家及工作小組成員於 12 人中包含 4 位女性參與及意見表達。專案執行團隊亦將邀請女性成員參與。
評估項目	**評估結果**
1-3【請根據 1-1 及 1-2 的評估結果，找出本計畫之性別議題】 性別議題舉例如次： **a.參與人員** 政策規劃者或服務提供者之性別比例差距過大時，宜關注職場性別隔離（例如：某些職業的從業人員以特定性別為大宗、高	1.本計畫在決審委員之組成，將會重視決審委員之性別組成。 2.本案於推動時，就專家及研究團體進行性別統計，關注參與

階職位多由單一性別擔任）、職場性別友善性不足（例如：缺乏防治性騷擾措施；未設置哺集乳室；未顧及員工對於家庭照顧之需求，提供彈性工作安排等措施），及性別參與不足等問題。 **b.受益情形** ①受益者人數之性別比例差距過大，或偏離母體之性別比例，宜關注不同性別可能未有平等取得社會資源之機會（例如:獲得政府補助；參加人才培訓活動），或平等參與社會及公共事務之機會（例如:參加公聽會/說明會）。 ②受益者受益程度之性別差距過大時（例如:滿意度、社會保險給付金額），宜關注弱勢性別之需求與處境（例如:家庭照顧責任使女性未能連續就業，影響年金領取額度）。 **c.公共空間** 公共空間之規劃與設計，宜關注不同性別、性傾向、性別特質及性別認同者之空間使用性、安全性及友善性。 ①使用性：兼顧不同生理差異所產生的不同需求。 ②安全性：消除空間死角、相關安全設施。 ③友善性：兼顧性別、性傾向或性別認同者之特殊使用需求。 **d.展覽、演出或傳播內容** 藝術展覽或演出作品、文化禮俗儀典與觀念、文物史料、訓練教材、政令/活動宣導等內容，宜注意是否避免複製性別刻板印象、有助建立弱勢性別在公共領域之可見性與主體性。 **e.研究類計畫** 研究類計畫之參與者（例如:研究團隊）性別落差過大時，宜關注不同性別參與機會、職場性別友善性不足等問題；若以「人」為研究對象，宜注意研究過程及結論與建議是否納入性別觀點。	決策之性別平等及科技人才性別衡平性等性別議題。

貳、回應性別落差與需求：針對本計畫之性別議題，訂定性別目標、執行策略及編列相關預算。

評估項目	評估結果
2-1【請訂定本計畫之性別目標、績效指標、衡量標準及目標值】 請針對 1-3 的評估結果，擬訂本計畫之性別目標，並為衡量性別目標達成情形，請訂定相應之績效指標、衡量標準及目標值，並納入計畫書草案之計畫目標章節。性別目標宜具有下列效益： **a.參與人員**	□有訂定性別目標者，請將性別目標、績效指標、衡量標準及目標值納入計畫書草案之計畫目標章節，並於本欄敘明計畫書草案之頁碼：

[1]促進弱勢性別參與本計畫規劃、決策及執行，納入不同性別經驗與意見。 [2]加強培育弱勢性別人才，強化其領導與管理知能，以利進入決策階層。 [3]營造性別友善職場，縮小職場性別隔離。 **b.受益情形** ① 回應不同性別需求，縮小不同性別滿意度落差。 ② 增進弱勢性別獲得社會資源之機會（例如:獲得政府補助；參加人才培訓活動）。 ③ 增進弱勢性別參與社會及公共事務之機會（例如:參加公聽會/說明會，表達意見與需求）。 **c.公共空間** 回應不同性別對公共空間使用性、安全性及友善性之意見與需求，打造性別友善之公共空間。 **d.展覽、演出或傳播內容** ① 消除傳統文化對不同性別之限制或僵化期待，形塑或推展性別平等觀念或文化。 ② 提升弱勢性別在公共領域之可見性與主體性（如作品展出或演出；參加運動競賽）。 **e.研究類計畫** ① 產出具性別觀點之研究報告。 ② 加強培育及延攬環境、能源及科技領域之女性研究人才，提升女性專業技術研發能力。 **f.**強化與本計畫相關的性別統計與性別分析。 **g.**其他有助促進性別平等之效益。	■未訂定性別目標者，請說明原因及確保落實性別平等事項之機制或方法。 1.本計畫研究團隊之女性研究人員比例約 5%。 2.本計畫諮詢、規劃及決審委員之女性委員，專家成員女性比例約 1/10。 3.本案持續關注不同性別參與諮詢、規劃及決審階段之情形，以努力朝向任一性別比例不少於三分之一原則。
評估項目	**評估結果**
2-2【請根據 2-1 本計畫所訂定之性別目標，訂定執行策略】 請參考下列原則，設計有效的執行策略及其配套措施： **a.參與人員** [1] 本計畫研擬、決策及執行各階段之參與成員、組織或機制（如相關會議、審查委員會、專案辦公室成員或執行團隊）符合任一性別不少於三分之一原則。 [2] 前項參與成員具備性別平等意識/有參加性別平等相關課程。 **b.宣導傳播**	■有訂定執行策略者，請將主要的執行策略納入計畫書草案之適當章節，並於本欄敘明計畫書草案之頁碼： 1. 本計畫在先期規劃諮詢專家及工作小組成員於 12 人中包含 4 位女性參與及意見表達。專案執行團隊亦將具有女性成員。

① 針對不同背景的目標對象（如不諳本國語言者；不同年齡、族群或居住地民眾）採取不同傳播方法傳布訊息（例如：透過社區公布欄、鄰里活動、網路、報紙、宣傳單、APP、廣播、電視等多元管道公開訊息，或結合婦女團體、老人福利或身障等民間團體傳布訊息）。 ② 宣導傳播內容避免具性別刻板印象或性別歧視意味之語言、符號或案例。 ③ 與民眾溝通之內容如涉及高深專業知識，將以民眾較易理解之方式，進行口頭說明或提供書面資料。 **c.促進弱勢性別參與公共事務** ① 計畫內容若對人民之權益有重大影響，宜與民眾進行充分之政策溝通，並落實性別參與。 ② 規劃與民眾溝通之活動時，考量不同背景者之參與需求，採多元時段辦理多場次，並視需要提供交通接駁、臨時托育等友善服務。 ③ 辦理出席民眾之性別統計；如有性別落差過大情形，將提出加強蒐集弱勢性別意見之措施。 ④ 培力弱勢性別，形成組織、取得發言權或領導地位。 **d.培育專業人才** ① 規劃人才培訓活動時，納入鼓勵或促進弱勢性別參加之措施 （例如:提供交通接駁、臨時托育等友善服務；優先保障名額；培訓活動之宣傳設計，強化歡迎或友善弱勢性別參與之訊息；結合相關機關、民間團體或組織，宣傳培訓活動）。 ② 辦理參訓者人數及回饋意見之性別統計與性別分析，作為未來精進培訓活動之參考。 ③ 培訓內涵中融入性別平等教育或宣導，提升相關領域從業人員之性別敏感度。 ④ 辦理培訓活動之師資性別統計，作為未來師資邀請或師資培訓之參考。 **e.具性別平等精神之展覽、演出或傳播內容** ① 規劃展覽、演出或傳播內容時，避免複製性別刻板印象，並注意創作者、表演者之性別平衡。 ② 製作歷史文物、傳統藝術之導覽、介紹等影音或文字資料時，將納入現代性別平等觀點之詮釋內容。	2. 計畫未來在研究團隊的部分，將會鼓勵團隊積極培育女性研究人員，顧及女性研究人員參與的比例。 □未訂執行策略者，請說明原因及改善方法：

③ 規劃以性別平等為主題的展覽、演出或傳播內容（例如:女性的歷史貢獻、對多元性別之瞭解與尊重、移民女性之處境與貢獻、不同族群之性別文化）。 **f.建構性別友善之職場環境** 委託民間辦理業務時，推廣促進性別平等之積極性作法（例如：評選項目訂有友善家庭、企業托兒、彈性工時與工作安排等性別友善措施；鼓勵民間廠商拔擢弱勢性別優秀人才擔任管理職），以營造性別友善職場環境。 **g.具性別觀點之研究類計畫** ①研究團隊成員符合任一性別不少於三分之一原則，並積極培育及延攬女性科技研究人才；積極鼓勵女性擔任環境、能源與科技領域研究類計畫之計畫主持人。 ②以「人」為研究對象之研究，需進行性別分析，研究結論與建議亦需具性別觀點。	
評估項目	**評估結果**
2-3【請根據 2-2 本計畫所訂定之執行策略，編列或調整相關經費配置】 各機關於籌編年度概算時，請將本計畫所編列或調整之性別相關經費納入性別預算編列情形表，以確保性別相關事項有足夠經費及資源落實執行，以達成性別目標或回應性別差異需求。	□有編列或調整經費配置者，請說明預算額度編列或調整情形： ■未編列或調整經費配置者，請說明原因及改善方法： 本計畫鼓勵研究團隊積極培育女性研究人員，顧及女性研究人員參與的比例。

【注意】填完前開內容後，請先依「填表說明二之（一）」辦理【第二部分－程序參與】，再續填下列「參、評估結果」。

參、評估結果

請機關填表人依據【第二部分－程序參與】性別平等專家學者之檢視意見，提出綜合說明及參採情形後通知程序參與者審閱。

3-1 綜合說明	本計畫於申請、審查、或執行均尊重不同性別，無限定性別皆可參與，並將持續留意人才培育及參與者之性別比例，減少性別落差。	
3-2 參採情形	3-2-1 說明採納意見後之計畫調	1.感謝委員對本計畫的肯定，本計畫將持續導入不同性別及多元性別的友善機制，以利性別平等的理念在資安議題中被重視。

	整（請標註頁數）	2.本計畫係資安領域計畫，在培育人才方面係透過多樣化交流分享活動，以鼓勵不同性別之科技人才皆有機會可了解領域。 3.本計畫將適時檢視資安領域中不同機構之性別圖像人才，以規劃人才培訓方向，感謝委員的建議。
	3-2-2 說明未參採之理由或替代規劃	無。

3-3 通知程序參與之專家學者本計畫之評估結果：

已於 年 月 日將「評估結果」及「修正後之計畫書草案」通知程序參與者審閱。

- **填表人姓名：李丹容 職稱：科員 電話：02-27377982 填表日期：113 年 5 月 15 日**
- **本案已於計畫研擬初期□徵詢性別諮詢員之意見，或□提報各部會性別平等專案小組（會議日期：____年____月____日）**
- **性別諮詢員姓名：__林春鳳__ 服務單位及職稱：**屏東縣基督教女青年會 常務理事 **身分：符合中長程個案計畫性別影響評估作業說明第三點第__2__款**（如提報各部會性別平等專案小組者，免填）

（請提醒性別諮詢員恪遵保密義務，未經部會同意不得逕自對外公開計畫草案）

【第二部分－程序參與】：由性別平等專家學者填寫

程序參與之性別平等專家學者應符合下列資格之一： ■1.現任臺灣國家婦女館網站「性別主流化人才資料庫」公、私部門之專家學者；其中公部門專家應非本機關及所屬機關之人員（人才資料庫網址:http://www.taiwanwomencenter.org.tw/）。 ■2.現任或曾任行政院性別平等會民間委員。 ■3.現任或曾任各部會性別平等專案小組民間委員。	
（一）基本資料	
1.程序參與期程或時間	113 年 5 月 16 日 至 113 年 5 月 17 日
2.參與者姓名、職稱、服務單位及其專長領域	林春鳳 屏東縣基督教女青年會 總幹事 休閒治療 休閒活動設計與帶領 體育行政 原住民族教育 性別主流化
3.參與方式	□計畫研商會議 □性別平等專案小組 ■書面意見
（二）主要意見（若參與方式為提報各部會性別平等專案小組，可附上會議發言要旨，免填 4 至 10 欄位，並請通知程序參與者恪遵保密義務）	
4.性別平等相關法規政策相關性評估之合宜性	理念上頗合宜，但在法規的連結上請具體地提出相關的法律及政策，此計畫與性別政策綱領之環境能源科技篇的關連比較強，請明列此政策之名稱。
5.性別統計及性別分析之合宜性	統計資料僅大略呈現數據及比例，建議更具體地說明百分比之情況。
6.本計畫性別議題之合宜性	合宜
7.性別目標之合宜性	合宜
8.執行策略之合宜性	合宜
9.經費編列或配置之合宜性	合宜
10.綜合性檢視意見	1。此為國家重要之國際競爭之計畫，不同性別的決策及參與在此領域有著明顯的差異，計畫內容亦提到將積極培育不同性別之科技人才投入相關之重要工程，建議具體明列如何與不同單位合作的方法及鼓勵內容。 2。人才培育與鼓勵的策略宜在計畫內按時間之期程有所作為，以利不同性別工作機會之產生，同時在工作的場域中強調不同性別及多元性別的友善機制，以利性別平等的理念在資安議題中被重視。

	3。人才的培育乃長期之運作工程，逐年的不同性別參與之統計資料為重要參考資訊，建議每年都要積極地統計在資安領域不同機構裡的性別圖像，以明確理解後續規劃之方向。
（三）參與時機及方式之合宜性	合宜
本人同意恪遵保密義務，未經部會同意不得逕自對外公開所評估之計畫草案。 （簽章，簽名或打字皆可）___林春鳳_____	

四、風險管理評估檢視表

下表資料填寫請參酌國發會公布之「行政院及所屬各機關風險管理及危機處理作業手冊」填寫。

【第一部分】：計畫現有風險圖像

嚴重 (3)			
中度 (2)	R=2 低度風險		
輕微 (1)			
影響程度 / 可能性	不太可能 (1)	可能 (2)	非常可能 (3)

【第二部分】：計畫風險評估及處理彙總表

風險項目	風險情境	現有風險對策	可能影響層面	現有風險等級		現有風險值(R)=(L)x(I)	新增風險對策	殘餘風險等級		殘餘風險值(R)=(L)x(I)
				可能性(L)	影響程度(I)			可能性(L)	影響程度(I)	
資安技術研發人才不足	資安問題日益嚴重，是重要研究議題之一，然業界待遇較學界優渥，資訊領域人才投入資安研究意願相對低落。	計畫內擴大鼓勵補助大專學生參與資安研究，於預算額度範圍內，吸引更多潛在資安研究人才投入資安技術研發。	我國資安人才供應出現斷層	2	1	2	-	2	1	2

【第三部分】：計畫殘餘風險圖像

嚴重 (3)			
中度 (2)	R=2 低度風險		
輕微 (1)			
影響程度 / 可能性	不太可能 (1)	可能 (2)	非常可能 (3)

低度風險： 1 項(100 %)

五、政府科技發展計畫審查意見回復表(A008)

審議編號：114-1901-11-20-01

計畫名稱：臺灣資安卓越深耕-學術型資安研究

申請機關(單位)：國科會前瞻處

序號	審查意見	回復說明	修正頁碼
1	(數位部資安署) 依據行政院訂頒「資安產業發展行動計畫」，各政府機關之中長程個案計畫應提撥一定比例經費辦理資安防護作業(計畫經費 1 億至 10 億(含)，提撥比例為 6%)；查本計畫資安經費提撥比例 100%，投入項目尚屬合理，符前揭資源投入要求。	感謝委員支持。	
2	(主計總處) 1.本計畫著重於提升國內資安研發技術及提高資安人才培訓能量，藉由產學合作及技術移轉，擴散資安研發能量，並透過移地研究、舉辦及參與國際會議，掌握國內外資安技術發展趨勢，以提升我國資安技術水平。 2.審查意見： (1) 查數位發展部 114-117 年「深化資安跨域整合聯防計畫」，屬跨部會整合型計畫，係辦理推動資安產業發展、提升通傳網路、培育資安人才、強化資安防禦機制等，係將研究成果發散於產業應用，鑑於該計畫未邀集國科會共同提報，為期本計畫研究	感謝委員支持，有關審查意見提到本計畫相關研究成果及與數位部等機關相關計畫之介接應用機制部分，補充說明如下： 1.在我國「資安即國安」的政策方針下，行政院為整體布局資安藍圖，透過臺灣資安卓越深耕計畫，由數位部、國科會及教育部跨部會共同推動，活絡資安產業、發展資安科技並育成資安人才。其中，數位部擴大企業資安投資，並掌握資訊關鍵技術發展及成立國家整體資通安全研究院；國科會深耕學術型資安研究，於學術研究攻頂拔尖；教育部則推動擴增資安師資，以驅動資安生態系統。綜上，各機關已進行業務妥適分工，爰數位部研提之計	

	成果得供接續應用，建請國科會補充說明本計畫相關研究成果，與數位部等機關相關計畫之介接應用機制。 (2) 查本計畫總經費 5 億 9,500 萬元，截至 112 年度已編列 3 億 8,500 萬元，累計執行 3 億 8,479 萬 7 千元，執行率 99.9%。為應其賡續推動業務實際需要，114 年度所需經費建議如數核列 7,500 萬元。	畫本會未與其共同提報。 2.承上，本會於本計畫著重推動學術研究攻頂拔尖，整體布局上中游資安學術科研，串接下游跨部會合作應用，聚焦關鍵議題研究，引導策略型國際資安學術合作，促進國際拔尖，延攬國際學者訪台並參與國內研究計畫執行，培育資安學術研究人才。相關成果可提供予各有關部會，協助各部會串接下游資安科研應用工作。	
3	(科技辦公室) 1.扣合「智慧國家方案(2021-2025 年)」及六大核心戰略之資安政策。 2. (1) 計畫核心目標：軟硬結合、資安創新；資安資源共享與場域淬鍊；國際接軌、共同合作，符合政策目標。 (2) 目標達成情形：110-112 年累計 368 項前瞻關鍵資安技術或機制研發、擴大培育高階資安技術研發人才達 932 人。提升國際能見度，累計發表國際論文 275 件。累計促成 87 件產學合作、3 件檢測與驗證服務與 2 件技術移轉，合計 92 件合作案共 7,856 萬)。 3.本(114)年度計畫為全程	感謝委員支持與建議，有關建議 3.對各項成果之後續發展進行追蹤分析，將依委員建議進行盤點及分析，惟針對追蹤資安技術之運用情形及人才就業調查部分，依據臺灣資安卓越深耕計畫之跨部會分工，數位部主責擴大企業資安投資，並掌握資訊關鍵技術發展及成立國家整體資通安全研究院，教育部推動擴增資安師資，以驅動資安生態系統，本會則深耕學術型資安研究，於學術研究攻頂拔尖，著重提供前瞻技術研究成果供各部會串接下游產業合作應用，爰未於計畫中規劃整合資安技術之運用情形及人才就業調查之工作，尚請諒察。	

	計畫期程之最後一年，建議對各項成果之後續發展進行追蹤分析，例如前瞻關鍵資安技術與數位部、資安院等單位進行跨部會合作應用之運用情形；所培育高階資安技術研發人才之就業情形等。		
4	(綜合意見) 1.本計畫規劃兩大分項計畫，包含前瞻處所推動之分項一「前瞻資安技術研究 (Security in Air & Security on Chip)」與前瞻處及國研院推動之分項二「資安科技擴散及共享服務」,整合資安攻防平台與雲服務基礎設施之資源提供給前瞻科技研發團隊運用，先前年度里程碑皆已達成，未來規劃亦符合政策需要。 2.計畫規劃之目標及關鍵成果如促成產學合作或技術移轉案 6 件、專利 5 件、技術報告 4 份、先進國家移地研究或邀請國際頂尖資安專家來台演講 3 場、推動 100 人以上全國性雲端資安攻防競賽等，延續前期計畫方向，關鍵成果與目標扣合度亦高。惟部分成果以執行指標件數、人次等展現，不易評估其執行品質。建議本計畫增加執行效益於預期關鍵成果中，以利展現推動	1.感謝委員支持。 2.感謝委員指導，有關增加執行效益於預期關鍵成果中之建議，本計畫係著重推動學術研究攻頂拔尖，將致力嘗試投稿頂尖研討會(資安領域 h5-index 前 5 名)，並努力牽線國際上具備頂會發表能力的學者與機構，或主辦頂會等作為計畫執行效益，以即時籌獲前瞻資安研究議題與快速的研究方法；另中程策略規劃目標擬以國外資安頂尖研究機構建立中長期合作的關鍵夥伴關係作為 milestones，以突顯本計畫推動成果與亮點。 3.感謝委員指導，有關目標達成評估及後續規劃已說明如前述 2.，另針對研究具體成果除既有之產學合作外，推廣更廣泛的產業應用之建議，目前係由數位部主責推動企業資安投資及掌握資訊關鍵技術發	

	成果與亮點，尤其所提資安科技研究中心布局資安中長期策略規劃目標達成評估與 milestones。 3.最後一年宜總結 5 年計畫作為、「建立臺灣成為資安科研關件夥伴」目標達成評估、後續規劃等宜有說明。且本計畫於最後階段應將研究具體成果除既有之產學合作外，推廣更廣泛的產業應用，此部分宜有更具體規劃之工作項目。 4.有關資源投入合理性及建議經費各細部計畫(前瞻資安技術研究、資安科技擴散及共享服務)114 年度經常支出皆合理。	展，本會將盤點本計畫資安研究成果，提供數位部串接下游合作應用。 4.感謝委員支持。	

註：主筆委員完成審查意見後，系統將主動發信通知，請於期限前至「政府科技計畫資訊網」填寫完成意見回復。

六、資安經費投入自評表(A010)

(如有填寫疑問，請逕洽行政院資安處 3356-8063)

部會			單位				
審議編號	計畫名稱	期程(年)	總經費(千元)(A)	資訊總經費(千元)(B)	資安經費(千元)(C)	比例[註1](D)	備註
110-1901-04-20-05	臺灣資安卓越深耕-學術型資安研究	110	125,000	125,000	125,000	100%	
111-1901-04-20-04	臺灣資安卓越深耕-學術型資安研究	111	125,000	125,000	125,000	100%	
112-1901-04-20-02	臺灣資安卓越深耕-學術型資安研究	112	135,000	135,000	135,000	100%	
113-1901-04-20-02	臺灣資安卓越深耕-學術型資安研究	113	135,000	135,000	135,000	100%	
114-1901-11-20-01	臺灣資安卓越深耕-學術型資安研究	114	75,000	37,500	37,500	100%	

資安經費投入項目

項次	年度	投入項目類別[註2]	投入項目	預估經費(千元)
1	110	C2	學術型資安研究	125,000
2	111	C2	學術型資安研究	125,000
3	112	C2	學術型資安研究	135,000
4	113	C2	學術型資安研究	135,000
5	114	C2	學術型資安研究	75,000
總計				595,000

備註：

1、 資安經費提撥比例係依計畫總經費(A)或資訊總經費(B)計算(可多計畫合併)，各計畫可依業務性質及實際需求於計畫執行年度分階段辦理。

1-1 109 年(含)前結束之計畫，其需達成資安經費比例(D)計算方式=(資安總經費(C)/資訊總經費(B))*100%，1 億(含)以下提撥 7%、1 億以上至 10 億(含)提撥 6%、10 億以上提撥 5%。

1-2 110-114 年(含)後結束之計畫，除前述資安經費比例，另配合行政院政策逐年提高資安經費比例至「資安產業發展行動計畫(107-114 年)」所訂 114 年預期達成目標。

2、 投入項目類別請用下列代號填寫：

2-1 系統開發

(A1) **依據資通安全管理法—資通安全責任等級分級辦法之**「資通系統防護需求分級原則」，完備「資通系統防護基準」之**各項措施。**

(A2) 推動「安全軟體發展生命週期(SSDLC)」，可參考行政院國家資通安全會報技術服務中心所訂「資訊系統委外開發 RFP 資安需求範本」。

(A3) 依據經濟部工業局所訂「行動應用 APP 安全開發指引」、「行動應用 APP 基本資安檢測基準」、「行動應用 APP 基本資安自主檢測推動制度」等，進行相關資安檢測作業。

2-2 軟硬體採購

(B1) 依據資通安全管理法—資通安全責任等級之公務機關應辦事項，建置必要之縱深防禦機制，含網路層(例如：防火牆、網站防火牆等)、主機層(例如：防毒軟體、電子郵件過濾機制等)、應用系統層等資安防護措施。

(B2) 推動國內認證/驗證規範，並將該產品通過之相關認證/驗證或符合相關規範納入建議書徵求說明書，例如：影像監控系統需符合影像監控系統相關資安標準，且經合格實驗室認證通過。

(B3) 各項設備應導入政府組態基準(Government Configuration Baseline，GCB)。

2-3 其他建議項目

(C1) 資安檢測標準研訂。

(C2) 新興資安領域(例如：5+2產業創新計畫)之資安風險與防護需求研究。

(C3) 新興資安領域之人才培育。

(C4) 編撰資安訓練教材。

其他資安相關項目(例如：推動「資安產業發展行動計畫」之四項策略-建立以需求導向之資安人才培訓體系、聚焦利基市場橋接國際夥伴、建置產品淬煉場域提供產業進軍國際所需實績、活絡資安投資市場全力拓銷國際)。

七、其他補充資料

無。