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：112-1901-04-20-02

（國科會前瞻處、工程處、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

（核定本）

計畫全程：110 年 01 月至 114 年 08 月

中華民國 111 年 08 月

目 錄

壹、基本資料及概述表(A003)

<table>
<tr><td>審議編號</td><td colspan="4">112-1901-04-20-02</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</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">國科會前瞻處、工程處、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，包含前瞻處及工程處所推動之分項一「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="2">計畫目標及預期關鍵成果</td><td rowspan="2">與部會科技施政目標之關聯</td></tr>
<tr><td>112 年度</td><td>113 年度</td></tr>
<tr><td>目標 1:軟硬結合、資安創新

關鍵成果 1: 針對未來新興應用軟硬體潛在資安威脅，開發對應前瞻創新資安防護技術。
*研發資安防護技術與機制 15 項，促成產學合作 15 件或技轉 3 件或總金</td><td>目標 1: 軟硬結合、資安創新

關鍵成果 1: 針對未來新興應用軟硬體潛在資安威脅，開發對應前瞻創新資安防護技術。
*研發資安防護技術與機制 20 項，促成產學合作 15 件或技轉 3 件或總金</td><td>國科會:
1:擘劃科技藍圖，引領國家科技發展
4: 創造科研價值，回應社會需求</td></tr>
</table>

	額達 700 萬以上。 關鍵成果 2: 透過前瞻資安技術研發過程，強化軟硬體資安研發能量。 *培育資安技術研發人才 125 人。	額達 800 萬以上。 關鍵成果 2: 透過前瞻資安技術研發過程，強化軟硬體資安研發能量。 *培育資安技術研發人才 125 人。	
	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。 *完成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。 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。 *推動1場100人以上全國性雲端資安攻防競賽活動。	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。 *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。 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。 *推動 1 場 100 人以上全國性雲端資安攻防競賽活動。	國科會: 1:擘劃科技藍圖，引領國家科技發展 2:深耕卓越研究，打底科技研發能量
	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。 *與先進國家資安研發機構進行學術交流或出席	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。 *與先進國家資安研發機構進行學術交流或出席國	國科會: 3:營造人才沃土，厚植臺灣科研人才資本

	國際會議，參與國際交流 1 場；參與或主導大型跨國資安研究計畫 2 案。 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。 *參與國際研討會發表論文 10 篇。	際會議，參與國際交流 1 場；參與或主導大型跨國資安研究計畫 3 案。 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。 *參與國際研討會發表論文 12 篇。	
預期效益	**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「資安科技研究中心」為目標，擬定上位研究主題並配合國家資安學術拔尖議題，串連學研深耕資安科研發展，提升國內資安產業研發技術水平；透過雲端資安攻防平台提供服務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。		
計畫群組及比重	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 _40_ % ■ 工程科技 _60_ %　□人文社會 ____ %　□科技創新 ____ %		
計畫類別	■ 前瞻基礎建設計畫		
前瞻項目	□ 綠能建設　■ 數位建設　□ 人才培育促進就業之建設		
推動 5G 發展	□ 是　■ 否		
資通訊建設計畫	□ 是　■ 否		
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		

<table>
<tr><td></td><td colspan="5">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">112 年 01 月 01 日 至 113 年 12 月 31 日</td></tr>
<tr><td>全程期間</td><td colspan="5">110 年 01 月 01 日 至 114 年 08 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>111</td><td colspan="4">125,000</td></tr>
<tr><td rowspan="15">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">112 年度</td><td>人事費</td><td>87,750</td><td>土地建築</td><td>0</td></tr>
<tr><td>材料費</td><td>18,625</td><td>儀器設備</td><td>0</td></tr>
<tr><td>其他經常支出</td><td>28,125</td><td>其他資本支出</td><td>500</td></tr>
<tr><td>經常門小計</td><td>134,500</td><td>資本門小計</td><td>500</td></tr>
<tr><td colspan="2">經費小計(千元)</td><td colspan="2">135,000</td></tr>
<tr><td rowspan="5">113 年度</td><td>人事費</td><td>87,750</td><td>土地建築</td><td>0</td></tr>
<tr><td>材料費</td><td>18,625</td><td>儀器設備</td><td>0</td></tr>
<tr><td>其他經常支出</td><td>28,125</td><td>其他資本支出</td><td>500</td></tr>
<tr><td>經常門小計</td><td>134,500</td><td>資本門小計</td><td>500</td></tr>
<tr><td colspan="2">經費小計(千元)</td><td colspan="2">135,000</td></tr>
<tr><td>部會施政計畫關鍵策略目標</td><td colspan="5">研究躍升卓越－深耕基礎研究，厚植科研人才，提升國際影響;</td></tr>
<tr><td>本計畫在機關施政項目之定位及功能</td><td colspan="5">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整體串連研究成果，將臺灣資安學術發展推向國際。</td></tr>
<tr><td>計畫架構說明</td><td colspan="5">依細部計畫說明</td></tr>
</table>

<table>
<tr><td rowspan="10"></td><td>細部計畫 1
名稱</td><td colspan="5">前瞻資安技術研究(Security in Air & Security on Chip)</td></tr>
<tr><td>112 年度
概估經費(千元)</td><td>77,000</td><td rowspan="2">計畫
性質</td><td rowspan="2">基礎研究</td><td rowspan="2">預定
執行
機構</td><td rowspan="2">國科會前瞻處、工程處</td></tr>
<tr><td>113 年度
概估經費(千元)</td><td>77,000</td></tr>
<tr><td>細部計畫
重點描述</td><td colspan="5">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 on Chip)。</td></tr>
<tr><td rowspan="2">主要績效指標
KPI
(請填寫此細部計畫之主要績效指標(至多 3 項))</td><td colspan="5">112 年主要績效指標：
1. 開發 15 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 700 萬以上。
2. 培育高階資安技術研發人才 125 人。
3. 參與國際頂尖研討會發表論文 10 篇。</td></tr>
<tr><td colspan="5">113 年主要績效指標：
1. 開發 20 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 800 萬以上。
2. 培育高階資安技術研發人才 125 人。
3. 參與國際頂尖研討會發表論文 12 篇。</td></tr>
<tr><td>細部計畫 2
名稱</td><td colspan="5">資安科技擴散及共享服務</td></tr>
<tr><td>112 年度
概估經費(千元)</td><td>58,000</td><td rowspan="2">計畫
性質</td><td rowspan="2">基礎研究</td><td rowspan="2">預定
執行
機構</td><td rowspan="2">國科會前瞻處、國家實驗研究院</td></tr>
<tr><td>113 年度
概估經費(千元)</td><td>58,000</td></tr>
<tr><td>細部計畫
重點描述</td><td colspan="5">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</td></tr>
</table>

<table>
<tr><td rowspan="3"></td><td></td><td colspan="3">境建構」以及「育才與國際合作鏈結」。</td></tr>
<tr><td rowspan="2">主要績效指標
KPI</td><td colspan="3">112 年主要績效指標：
1. 促使 10 組研發團隊使用整合軟體資源服務。
2. 辦理 2 次資安產學研高峰座談。
3. 推動 100 人以上全國性雲端資安攻防競賽活動。
4. 資安尖端研究中長期戰略規劃報告 1 份。
5. 參與或主導大型跨國資安研究計畫 2 案</td></tr>
<tr><td colspan="3">113 年主要績效指標：
1. 促使 15 組研發團隊使用整合軟體資源服務。
2. 辦理 2 次資安產學研高峰座談。
3. 推動 100 人以上全國性雲端資安攻防競賽活動。
4. 資安尖端研究中長期戰略規劃報告 1 份。
5. 參與或主導大型跨國資安研究計畫 3 案</td></tr>
<tr><td>前一年計畫或相關之前期程計畫名稱</td><td colspan="4">臺灣資安卓越深耕-學術型資安研究(2/5)</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，累計 64 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 300 人。
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，辦理資安攻防實務人才培訓共計 9 場次累計 227 人次。
3. 提升國際能見度，累計發表國際論文 66 件。(國際研討會: 27 件、國外重要期刊: 30 件、國外一般期刊: 9 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 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 件合作案共 1,365 萬。</td></tr>
<tr><td rowspan="4">跨部會署計畫</td><td colspan="4">□ 是 ■ 否 （若屬跨部會合作計畫，請續填說明。）</td></tr>
<tr><td rowspan="2">合作部會署 1</td><td rowspan="2"></td><td>112 年度經費
(千元)</td><td></td></tr>
<tr><td>113 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>112 年度經費
(千元)</td><td></td></tr>
</table>

			113 年度經費 (千元)	
	負責內容	總字數 300 字內		
中英文關鍵詞	資通訊安全、晶片安全、前瞻研究、新興科技驗證場域、人才培育、國際合作。 security in air, security on chip, foresight research, emerging technology verification field, talents cultivation, international collaboration			
計畫連絡人	姓名	江紹平	職稱	科員
	服務機關	國科會前瞻處		
	電話	02-27377982	電子郵件	spchiang@nstc.gov.tw

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。

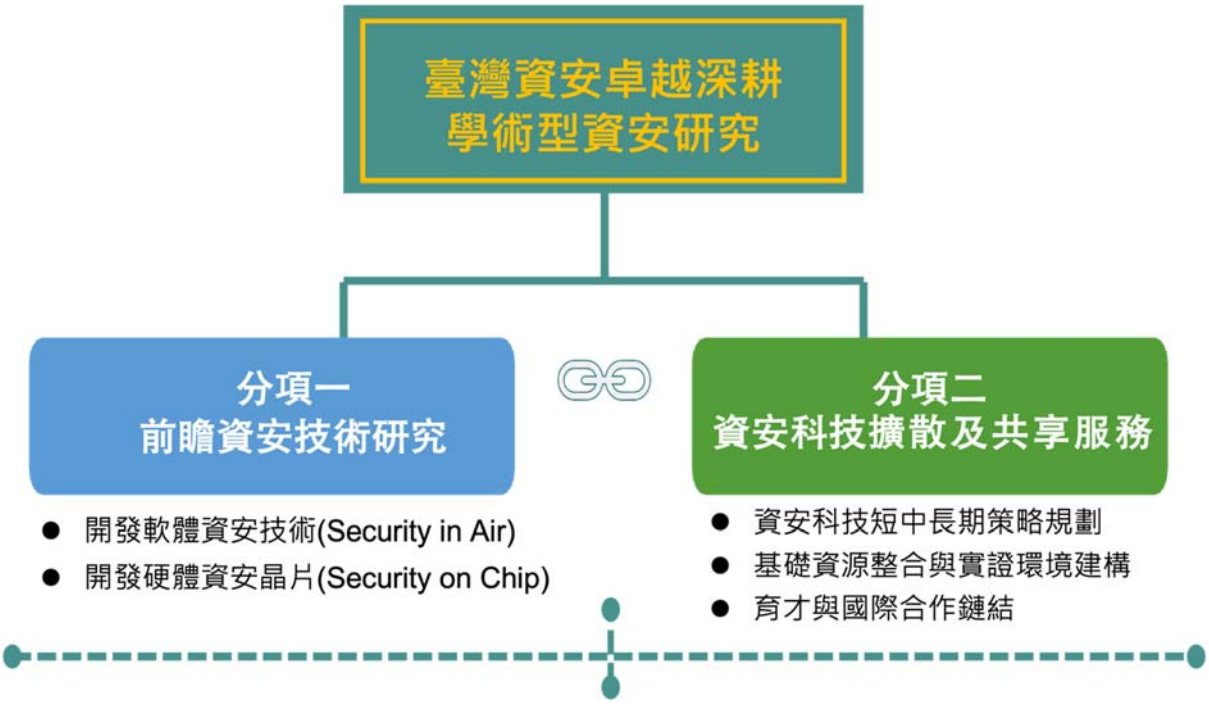

圖 1、計畫架構

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。

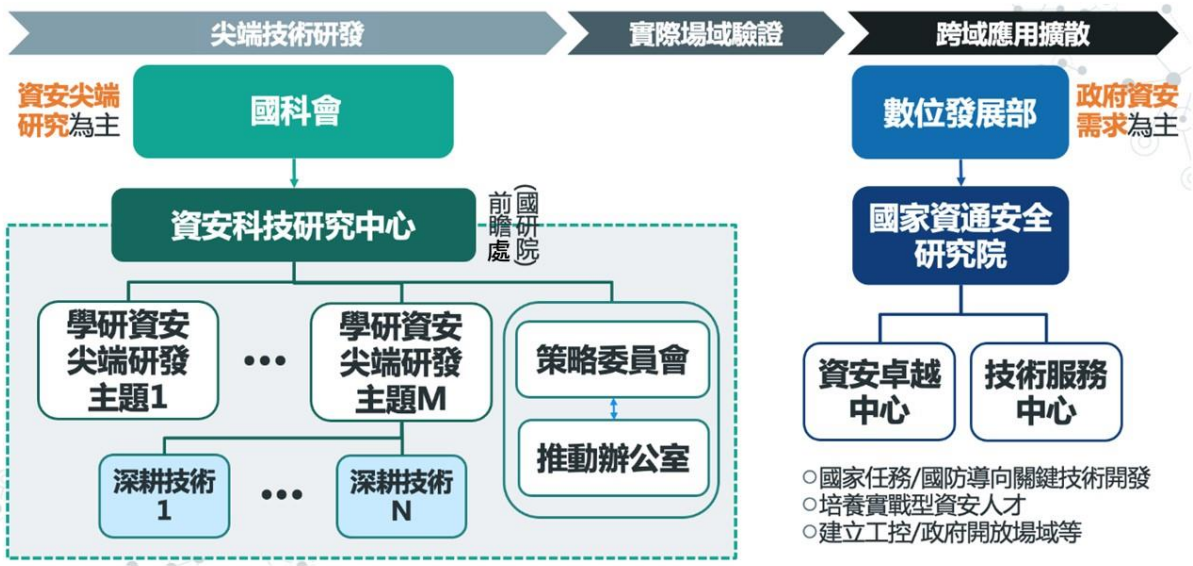

圖 2　資安科技研究中心運作架構

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。

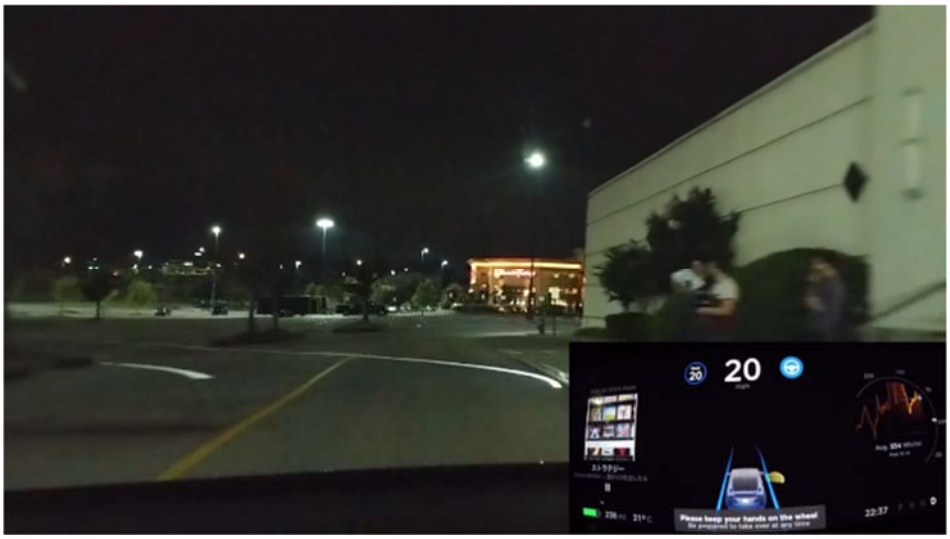

圖 4 誤導自駕車實驗

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：

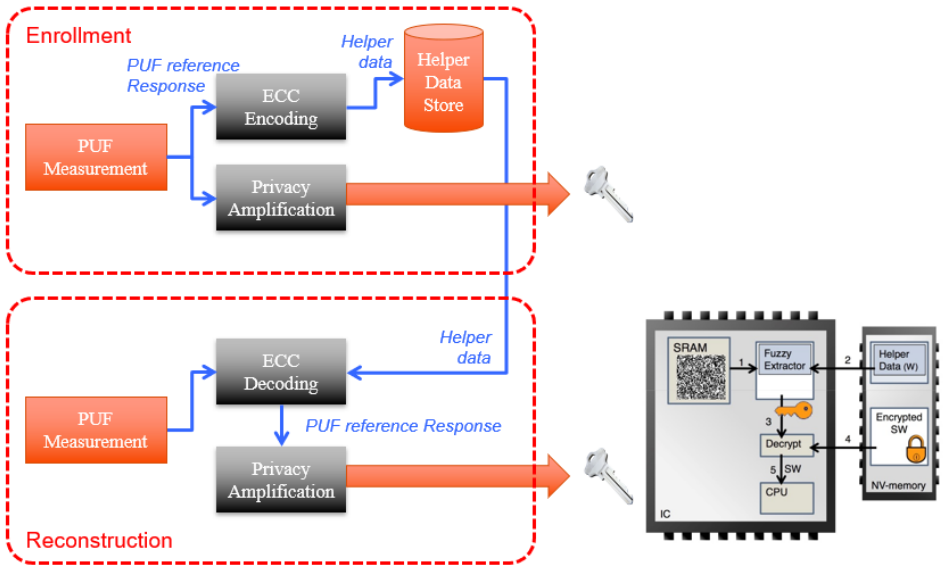

圖 5、應用 PUF 技術進行裝置認證示意圖

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。

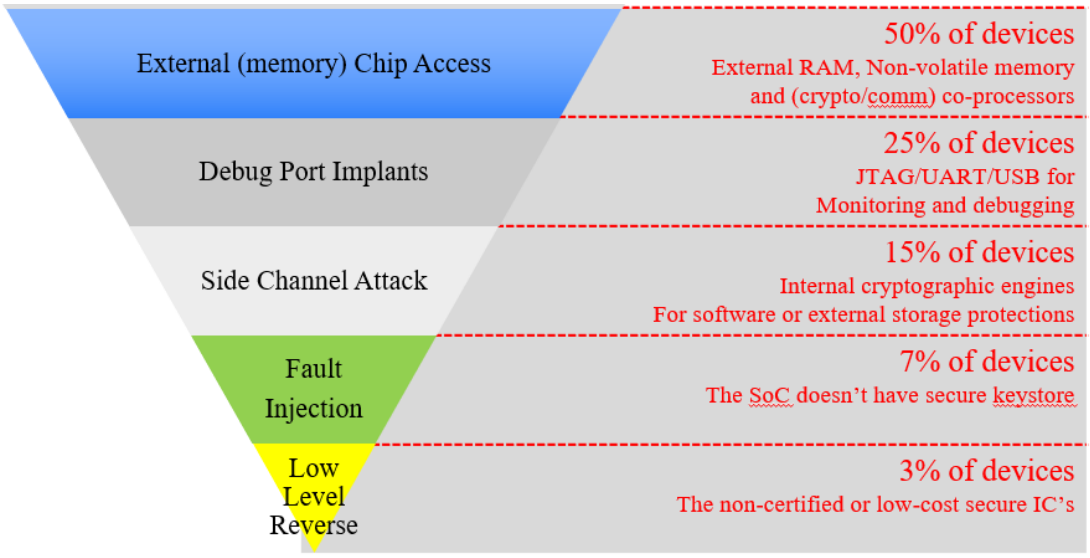

圖 6、實體裝置攻擊手法分析

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。

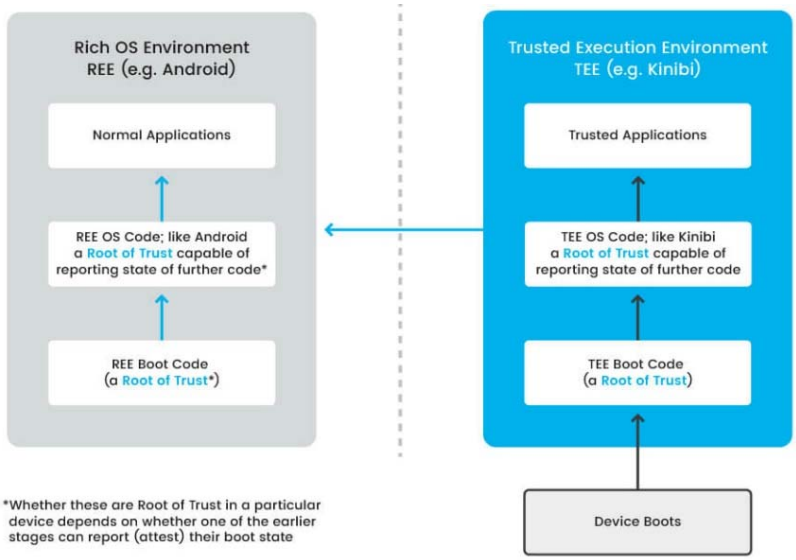

圖 7、可信任執行環境與其他系統環境

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。

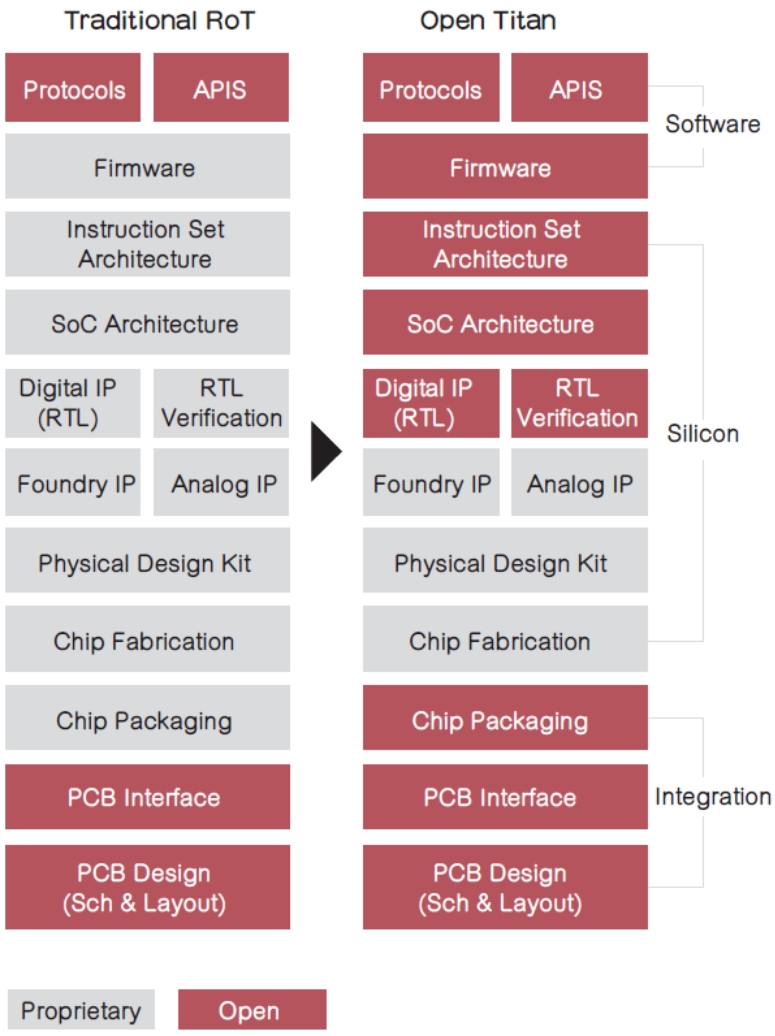

圖 8、傳統 RoT 與 OpenTitan RoT 主要設計比較

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。

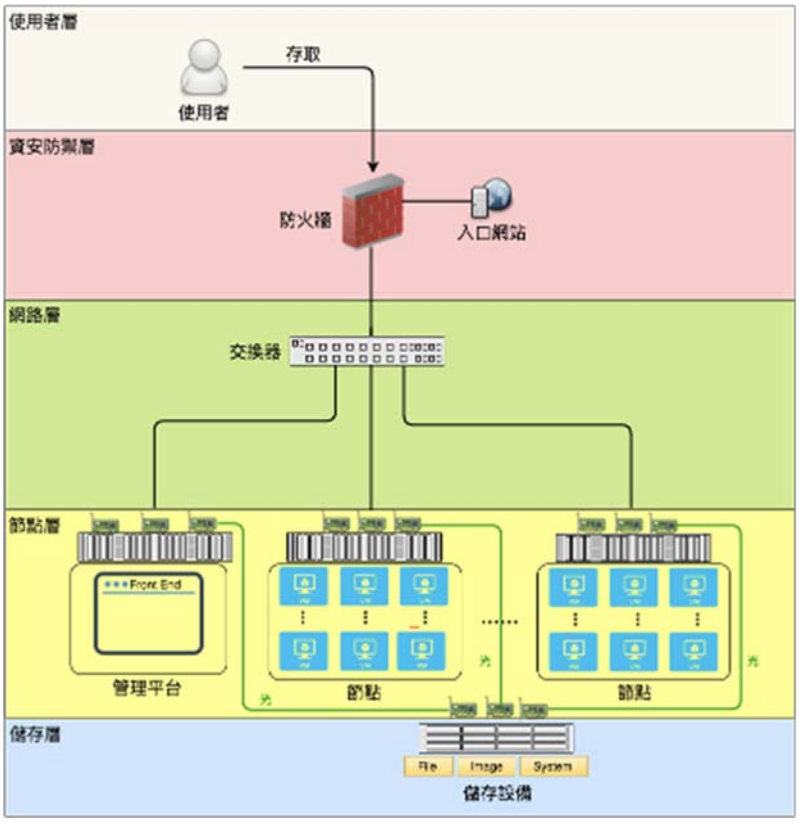

圖 11 平台簡易架構

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，以及網路拓撲圖的呈現，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

一、 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	1. 開發 10 項前瞻關鍵資安技術或機制，促成產學合作 15	1. 開發 15 項前瞻關鍵資安技術或機制，促成	1. 開發 20 項前瞻關鍵資安技術或機制，促成	1. 促成產學合作或技術移轉案 6 件或總金額達

	件或技轉 3 件或總金額達 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。	件或技轉 3 件或總金額達 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。	產學合作案 15 件或技轉 3 件或總金額達 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	產學合作案 15 件或技轉 3 件或總金額達 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	300 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. 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	1. 累計 64 項前瞻關鍵資安技術或機制研				

(重大效益)	發進行中，累計促成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件合作案共 1,365萬。 2. 培育高階資安技術研發人才達300人。 3. 累計發表國際論文66件。(國際研討會:27件、國外重要期刊:30件、國外一般期刊:9件)。 4. 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。 5. 辦理資安攻防演練9場次。 6. 資安專業實務人才培訓 227人次。				

二、 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) ● 針對 5G(B5G)、IoT 與 AI 等相關應用潛在威脅，開發對應前瞻資安防護技術 ● 開發先進資安技術與防護機制，培育資安研發人才，建立資安研發自主能量 ● 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 ● 建構資安基礎整合環境 (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

三、 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。

四、 與以前年度差異說明

多年期計畫請簡扼說明每年度差異之處，差異項目可為年度階段性目標、執行重點、績效指標等。

年度 差異項目	110-111 年度	112-113 年度
資安科技整合與研究	110 年: CDX (Blue Team、Red Team Offense)	112 年: 國家資安策略規劃及整合含雲端資安攻防平台之共享研發資源
	111 年：CDX(IoT 、 Bank Hacking)	113 年: 國家資安策略規劃及整合含雲端資安攻防平台之共享研發資源
培育高階資安技術研發人才	250 人	250 人

五、 跨部會署合作說明

本計畫無。

六、 與本計畫相關之其他預算來源、經費及工作項目

(請依 112、113 年度拆分說明)

預算來源	經費(千元)	工作項目
科技發展		
公共建設		
基本需求 (部會施政+社會發展)		
其他(如作業基金)		

本計畫無。

肆、前期重要效益成果說明

一、110 年度重要執行成果

(一)【前瞻資安技術研究(Security in Air & Security on Chip)】

1. 人工智慧時代的硬體安全：威脅與防護: 使用深度學習研發自動防禦旁通道攻擊的技術，採用美國 NIST 所建議的旁通道洩溢檢測法：TVLA，藉由統計分析旁通道訊號中的洩溢量是否超標來評估晶片的安全；並分析各種硬體攻擊方法及硬體安全弱點，以提供增進晶片安全的對策。(中興大學&資策會產學合作2件160萬)
2. 物聯網端點的韌體之動靜態混合分析與檢測: 採用符號分析與安全的韌體技術，建立物聯網韌體與週邊設備自動模擬，並將模擬的風險訊息提供車控組提前應對，以下降韌體的資安風險，提高自駕車系統的可用性與安全性。(臺科大&工研院產學合作100萬)
3. PUF-based 軟硬整合資安晶片技術: 使用機器學習技術針對工控系統的異常流量進行偵測，研發工控系統的異常流量防禦技術。(臺大&資策會產學合作1件70萬)
4. 智慧製造機聯網之動態密碼資安技術及落地驗證: 以未來網路通訊加密技術應用的關鍵加密技術的亂數產生器設計，利用混沌理論之亂數產生器，結合系統控制理論，完成同步控制器之設計。(成大技轉給傑睿資訊1件50萬)
5. 智慧政府骨幹之主動式安全與隱私延伸保護技術框架: 採用 Kubernetes (簡稱為 K8s) 安全服務建置技術，開發客製化管理工具，產出一套符合安全的硬體資源共享系統。(台科大&撼訊科技產學合作1件200萬)
6. PUF-based 軟硬整合資安晶片技術: 建立勒索軟體攻擊腳本與應變計畫(SOP)，強化勒索軟體的防禦應變。(台大&總統府產學合作1件96萬)
7. 智慧製造機聯網之動態密碼資安技術及落地驗證: 確保網站運作與管理維運能符合資安法規需求，協助經濟部能源局網站，進行網站功能新增改版與系統資安維護作業，以及針對電業登記網站資料移轉與系統功能進行維護作業。(成大&工研院產學合作2件160萬)
8. 水資源關鍵基礎設施資安防護: 協助產業辦理智慧製造和資訊管理人才培訓課程。(成大&宏致電子產學合作1件136萬)
9. 積極展現臺灣資安實力，提升我國資安領域能見度，並有2件參加國際研討會發表，榮獲 Best Paper Award。
   (1) AsiaJCIS 2021「Best Paper Award」,Aug. 19-20, 2021 in Seoul, Korea
   * 發表論文主題: Improved Proxy Re-encryption Scheme with Equality Test
   * 作者: Chih-Chen Yang, Raylin Tso, Zi-Yuan Liu, Jen-Chieh Hsu, Yi-Fan Tseng

(2) ICSEVEN 2021 「Best Paper Award」,Oct. 28-31, 2021 in Taitung, Taiwan
   * 發表論文主題: Design a Telemedicine System in Rural Areas Using Blockchain Technology
   * 作者: Ma. Thea A. Cabral; N.Y. Lee

10. 累計培育專業資安證照人才43人:
   (1) IEC 62443_13人
   (2) ISO 27001 LAC_5人
   (3) ISO/IEC 27701:2019_1人
   (4) eLearnSecurity Junior Penetration Tester_ 1人
   (5) EC-Concil Certified Ethical Hacker_ 1人
   (6) ICDL IT Security_ 7人
   (7) Microsoft Certified Security, Compliance, and Identity Fundamentals_ 9人
   (8) Microsoft Certified Azure Data Fundamentals_ 6人
11. 累計培育專業資安講師證照人才1人(Cisco DevNet Associate)。

(二)【雲端資安攻防平台(CDX)】

1. 完成攻防演練賽制與評分方式規劃，將採用紅軍及藍軍的擬真企業場景，搭配即時監控機制檢核參賽人員資安防護之情形，並納入計分機制及整合視覺化計分版。
2. 新興科技擬真攻防場域開發: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，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。(國網中心&精誠資訊 / 產學合作80萬)

二、里程碑達成情形

(一)【O1】軟硬結合、資安創新：

1. 【KR1】針對未來新興應用軟硬體潛在資安威脅，開發對應前瞻創新資安防護技術。研發資安防護技術與機制10項，促成產學合作15件或技轉3件或總金額達600萬以上。達成情形如下：
   (1) 經期中審視調整部分項目之研發內容，調整後累計共64項前瞻關鍵資安技術或機制研發進行中。(24項關鍵技術、8項檢測技術、12項應用平台、5項整合方案與15項基礎理論)。

(2) 累計促成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件合作案共1,365萬。

2. 【KR2】透過前瞻資安技術研發過程，強化軟硬體資安研發能量。培育資安技術研發人才125人。達成情形如下：

累計培育高階資安技術研發人才300人。(博後: 8、專任(碩):16、碩士生: 246、博士生: 30)

(二) 【O2】資安場域、淬鍊技術：

1. 【KR1】針對未來產業新興科技應用，進行特定領域資安實證場域研究。建置新興科技資安攻防實證場域2項(Blue Team、Red Team Offense)。達成情形如下：

(1) BlueTeam 專屬場域與演練場景的建置與設計方案持續進行中。

(2) 已在場域主機上佈建五種漏洞，目前正進行 Red Team Offense 攻擊測試、Blue Team 防禦測試與修補方式測試。並已將預先蒐集的測試程式用於測試弱點主機，藉由藍隊場域進行攻擊場域腳本規劃。 後續將持續進行環境整合與配合劇本場景之規劃，陸續佈建於 CDX 環境，並且配合 Red Team 之攻擊手法設計，進行主機佈建優化。

(3) 完成攻防演練賽制與評分方式規劃，將採用紅軍及藍軍的擬真企業場景，搭配即時監控機制檢核參賽人員資安防護之情形，並納入計分機制及整合視覺化計分版。

(4) 開發與調校產業場域: 已完成 Red Team 場域環境及攻擊手法研究，並於 Red Team 場域預先收集測試程式，用以測試弱點主機。另外將藉由藍隊場域進行攻擊場域的腳本規劃，以持續進行環境整合與測試攻擊程式。

2. 【KR2】利用自建新興科技資安攻防實證場域，淬鍊特定領域資安技術。新興科技資安攻防實務人才培訓90人次。新興科技資安攻防演練1場。達成情形如下：

新興科技資安攻防實務人才培訓共計辦理9場次，累計227人次：

(1) 2021年3月25日至26日辦理竹科廠商 Blue Team 資安人才培訓，共計20人次。 (金士頓科技股份有限公司)

(2) 2021年4月9日在雲林科技大學舉辦兩場 Workshop(CDX 教學應用工作坊、CDX 競賽應用工作坊)，出席人數共54人次。

(3) 2021年10月6、13日在高鐵桃園訓練中心舉辦兩場企業網路攻防實務(合作企業:台灣高鐵)，出席人數共40人次。

(4) 2021年11月3、4日在台北文創舉辦資安攻防競賽決賽(合辦企業:精誠集團，參與決賽人數：共12隊，每隊4人)。

(5) 2021年11月6、13日辦理高鐵公司資安人才培訓，共計65人次。(委辦企業:台灣高鐵)

(三) 【O3】國際接軌、共同合作：

1. 【KR1】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。與先進國家資安研發機構進行學術交流或出席國際會議，參與國際交流1場。達成情形如下：

   因應 COVID-19疫情影響，目前國際會議均採線上會議方式進行，已累計參與國際線上會議進行國際交流13場：(原訂為2021/12/31完成查核點項目，目前已超前進度)

   (1) SIBCON 2021, May 13-15
   (2) IEEE ECBIOS 2021, May 28-30
   (3) ICAI 2021， July 26-29
   (4) AsiaJCIS 2021, Aug. 19-20
   (5) IEEE COINS 2021, Aug. 23
   (6) AWASN'21, Aug.9-12
   (7) ICSEVEN 2021,Oct. 28-31
   (8) ICMU 2021,Nov.17-19
   (9) SITAIBA 2021,Nov. 18-20
   (10) ISPACS 2021,Nov. 16-19
   (11) CANDAR 2021, Nov. 23-26
   (12) ISNST 2021,Nov.18-19
   (13) IEEE ICEIB 2021 ，Dec. 10-12

2. 【KR2】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。參與國際研討會發表論文8篇。達成情形如下：

   積極展現臺灣資安實力，提升我國資安領域能見度，累計發表國際論文66件，並有2件參加國際研討會發表，榮獲 Best Paper Award。(國際研討會: 27件、國外重要期刊: 30件、國外一般期刊: 9件)

三、可量化經濟效益

110 年特別預算創造工作機會與帶動公民營企業投資

創造工作機會	帶動公民營企業投資(萬元)
0	1,445

(一)創造就業機會

1. 無。

(二)帶動公民營企業投資共 18 件，投資金額達 1445 萬元。

1. 資策會 3 件 230 萬
2. 工研院 4 件 355 萬
3. 國泰金控 1 件 100 萬
4. 盛群半導體 1 件 85 萬
5. 日本 Kioxia 1 件 87 萬
6. 撼訊科技 1 件 200 萬
7. 總統府 1 件 96 萬
8. 宏致電子 1 件 136 萬
9. 矽方科技 ISO 16845 驗證 1 件 4 萬
10. 泓格科技 IEC 62443-3-3 驗證 1 件 12 萬
11. 北晟有限公司 CAN Bus 封包檢測 1 件 10 萬
12. 傑睿資訊 1 件 50 萬
13. 精誠資訊 1 件 80 萬

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

請說明計畫之預期效益(效益與初級產出不同，效益指計畫對利益關係人或對社會經濟的影響) 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

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。
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。
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。
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。
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。
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。

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。
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。
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。
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。
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。
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

(請附 110 年度及 111 年度挑戰目標及達成情形)

110 年度挑戰目標及達成情形

挑戰目標：

1. 研發 IoT、5G、AI、網路安全、關鍵基礎設施、晶片安全等相關之關鍵資訊

安全技術與防護機制，期能與國際接軌。

2. 培育關鍵資安技術研發與頂尖人才，增加資安新創能量。
3. 與國內外資安廠商合作，將產品導入至雲端資安攻防平台實戰場域中，以協助進行產品功能及安全性的驗證。
4. 與國內廠商共同舉辦或參與台灣資安週活動。

達成情形說明：

1. 研發 IoT、5G、AI、網路安全、關鍵基礎設施、晶片安全等相關之關鍵資訊安全技術與防護機制，累計 64 項前瞻關鍵資安技術或機制研發進行中，將持續努力，期能與國際接軌。
2. 擴大培育高階資安技術研發人才達 300 人，增加資安新創能量。
3. 與精誠等企業合作，將雲端資安攻防平台導入至企業產品組合中，以協助企業發展資安服務。然尚未與國內外資安廠商合作，將產品導入至雲端資安攻防平台實戰場域中，以協助進行產品功能及安全性的驗證，後續將持續努力。
4. 110 年 5 月 4-6 日參與 iThome 舉辦的國內資安大會(CYBERSEC 2021 臺灣資安大會)。

111 年度挑戰目標

1. 研究國際共通性關鍵基礎設施防護規範。
2. 開發 IoT、5G 及 AI 等應用之資安工具。
3. 培育關鍵資安技術研發人才與晶片資安研發人才，厚實我國資安自主研發基礎。
4. 鼓勵國內學者加入國際頂級資安研討會議程委員，如 IEEE Symposium on Security and Privacy、ACM Conference on Computer and Communications Security、USENIX Security Symposium 等。
5. 與國內廠商共同舉辦或參與台灣資安週活動。。

達成情形說明：

專案執行中。

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	112 年度			113 年度			114 年度(8 月)		
		小計	經常支出	資本支出	小計	經常支出	資本支出	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	77,000	77,000	0	77,000	77,000	0	40,000	40,000	0
細部計畫 2:資安科技擴散及共享服務	基礎研究	58,000	57,500	500	58,000	57,500	500	35,000	33,000	2,000

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。

112 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。

112 年度經費需求表

單位：千元

計畫名稱	細部計畫重點描述	主要績效指標 KPI	112 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. 開發 15 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 700 萬以上。 2. 培育高階資安技術研發人才 125 人。 3. 參與國際頂尖研討會發表論文 10 篇。	77,000	57,750	9,625	9,625	0	0	0
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. 促使 10 組研發團隊使用整合軟體資源服務。 2. 辦理 2 次資安產學研高峰座談。 3. 推動 100 人以上全國性雲端資安攻防競賽活動。 4. 資安尖端研究中長期戰略規劃報告 1 份。 5. 參與或主導大型跨國資安研究計畫 2 案。	58,000	30,000	9,000	18,500	0	0	500

113 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。

113 年度經費需求表

單位：千元

計畫名稱	細部計畫重點描述	主要績效指標 KPI	113 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. 開發 20 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 800 萬以上。 2. 培育高階資安技術研發人才 125 人。 3. 參與國際頂尖研討會發表論文 12 篇。	77,000	57,750	9,625	9,625	0	0	0
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. 促使 15 組研發團隊使用整合軟體資源服務。 2. 辦理 2 次資安產學研高峰座談。 3. 推動 100 人以上全國性雲端資安攻防競賽活動。 4. 資安尖端研究中長期戰略規劃報告 1 份。 5. 參與或主導大型跨國資安研究計畫 3 案。	58,000	30,000	9,000	18,500	0	0	500

經費分攤表(B008)

112 年度

跨部會 主提/合提機關 (含單位)	細部計畫名稱	負責內容	主要績效指標 KPI	經費額度
經費合計				

無

經費分攤表(B008)

113 年度

跨部會 主提/合提機關 (含單位)	細部計畫名稱	負責內容	主要績效指標 KPI	經費額度
經費合計				

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，嗣後應依規定另送國科會審查)

本計畫無此事項

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
112	1								
	2								
	3								
	4								
	5								
	6								
總計									
113	1								
	2								
	3								
	4								
	5								
	6								
總計									

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：_____

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。