前瞻基礎建設－數位建設

強化國家資安基礎建設計畫
(核定本)

行政院資通安全處

106 年 7 月

目錄

壹、計畫緣起

隨著大數據、物聯網、移動裝置及雲端服務等新興資通訊科技應用普及，網路與實體世界已逐漸融合，新興資通訊科技固然對人類帶來生活的便利，然而伴隨而來的卻是衍生的資安風險，其對於民眾生活、經濟活動及國家安全的影響將與日俱增。

近年來，關鍵基礎設施的保護議題，已逐漸為各國所重視，主因在於關鍵基礎設施之防護完備與否，攸關國家安全、政府運作、人民生活、經濟發展與永續生活，依據行政院 103 年 12 月 23 日頒布之「國家關鍵基礎設施防護指導綱要」，我國關鍵基礎設施（CI）分類，採三層架構。第一層為主部門（Sector），第二層為次部門（Sub-sector），第三層為重要元件設施，詳述如下：

(一)主部門：分為能源、水資源、通訊傳播、交通、銀行與金融、 緊急救援與醫院、中央與地方政府機關、高科技園區 等八類。

(二)次部門： 依主部門重要元件之屬性再區分次部門，例如能源主 部門下再區分電力、石油、天然氣、化學與核能材料等次部門。

(三)重要元件設施： 係指維持設施營運所必須之重要設備、運作系統、通訊系統、維安系統，以及重要資訊系統或控制、調度 系統等。

前述各類關鍵基礎設施因應資通訊科技發展與潮流，多已應用或導入資通訊系統，用以控制關鍵基礎設施之日常運作，而此揭資通訊系統一旦遭受有心人士之惡意攻擊，將嚴重影響關鍵基礎設施之持續運作，爰此，「資安即國安」已為政府宣示之重要政策，為達前述政策目標，本計畫將著重關鍵資訊基礎設施之資安防護，全面打造數位國家所需之資安基礎建設，做為我國發展數位國家之後盾。

貳、計畫目標

本計畫與刻正規劃之第五期國家資通安全發展方案緊密銜接，規劃以「打造

安全可信賴的數位經濟時代」為願景，並以「厚植自我防護能量，保衛數位國家安全」為目標，並透過「完備資安基礎環境」、「建構國家資安聯防體系」、「推升資安產業自主能量」、「孕育優質資安人才」4 項策略，推動執行各項工作，針對「建構國家資安聯防體系」之關鍵資訊基礎設施資安防護，舉凡金融、通訊、政府服務、能源(水、電、油、瓦斯)、緊急救援、交通等關鍵基礎設施，本計畫編列特別預算，優先完成能源、通訊、政府骨幹網路等重要關鍵資訊基礎設施之資安防護建置，符合數位建設主軸一：推動資安基礎建設提供網路安心服務，提升全國資訊與資安環境，保障國家及人民安全，第五期發展方案 4 項策略，詳述如下：

一、 完備資安基礎環境

(一) 推動資通安全管理法及調適相關法規。

(二) 訂定資通安全相關標準、技術規範。

(三) 發展國家資通安全風險評估方法與策略。

(四) 建構寬頻網路及萬物連網所需之資通安全基礎建設。

二、 建構國家資安聯防體系

(一) 推動關鍵資訊基礎設施資安防護，發展防護基本政策與防護基準，並建立重要關鍵資訊基礎設施領域之資安資訊分享及分析中心(ISAC)、資安通報應變中心(CERT)及資安監控中心(SOC)。

(二) 建構預防暨打擊網路犯罪前端犯罪資料統合平台，強化偵辦網路駭侵案件偵辦能量。

(三) 提供警察機關資安事件及網路犯罪偵防與鑑識人才與能量，建置「跨域鑑識服務平台」、「網路犯罪資訊調查平台」及「網路犯罪與鑑識服務資源分享中心」，達成資源分享之目標。

(四) 開展多層次與多邊國際合作關係，促進跨國資安情資分享與交流。

三、 推升資安產業自主能量

(一) 完備資安產品認驗證機制。

(二) 擴大內需市場扶植資安產業升級與轉型。

(三) 鍊結產學研能量，深耕資安前瞻暨應用技術研發。

四、 孕育優質資安菁英人才

(一) 鼓勵大專院校開設資安學程，並推動中小學將資安素養議題融入課程教學。

(二) 拔擢在職資安優秀人才，進行資安精英人才培育

(三) 培育政府機關資訊與資安專職人才。

參、執行策略及方法

一、計畫期程：民國 106-109 年。

二、計畫經費與來源：特別預算 6 億元。

三、預定執行機關：經濟部、國發會、通傳會。

四、重點工作：

本計畫從國家整體資安之防禦面、人才面、技術面及產業面等面向出發，全面打造數位國家所需之資安基礎建設，做為我國發展數位國家之後盾。其

經費來源，原自科發基金管理會計畫補助款，但因該經費性質多屬經常門性質，惟資安之建設有部分係屬設備採購，故以特別預算 6 億資本門支應，規劃由 106 至 109 年度完成經濟部之水資源關鍵設施升級及安全管理、通傳會之數位匯流資通安全分析管理平臺及國發會之政府骨幹網路資安防護等，並分年建置前揭關鍵資訊基礎設施之資訊分享及分析中心(ISAC)、資安通報應變中心(CERT)及資安監控中心(SOC)，總體策略以結合相關部會，完備資安產品認驗證機制、擴大內需市場、扶植資安產業升級與轉型及鏈結產學研能量，深耕資安前瞻暨應用技術研發等，推升資安產業自主能量，主要用於通訊網路、能源、政府網路等關鍵資訊基礎設施之資安防護，並建立資安資訊分享及分析中心(ISAC)、資安通報應變中心(CERT)及資安監控中心(SOC)等用途，以加速建立重要關鍵資訊基礎設施提供者之資安緊急應變能量。

本計畫分別由經濟部、通傳會、國發會等機關共同執行，各別計畫內容詳附件 1 至附件 3。

一、經濟部：

推動關鍵基礎設施資安防護，強化水資源領域之關鍵資訊基礎設施資安防護，並建置經濟部關鍵資訊基礎設施領域之資安資訊分享及分析平台(E-ISAC) ，以強化資安聯防。

二、國發會：

依據行政院國家資通安全會報設置要點，主責政府網際服務網(GSN)骨幹網路及政府共構機房之維運，並提供政府骨幹網路資訊安全監控防護機制，透過事前偵測阻擋惡意訊息或攻擊及事後分析，有效提升政府網路安全，

確保政府提供為民服務網站穩定性及可用性，提高民眾滿意度，透過區域聯防之形式，持續監控分析全球之惡意活動與異常 IP，以最少資源達到聯合防禦的資安防護效果，統一部署及建置共通性資訊安全防禦機制，減少基層機關資安人力及預算不足問題。

三、通傳會：

依據主計總處 106 年 6 月 16 日召開之「前瞻基礎建設計畫第 1 期特別預算案籌編相關事宜會議」前瞻基礎建設-數位建設-強化國家資安基礎建設計畫辦理本項計畫，監管通訊傳播網路，強化通傳事業關鍵基礎設施之資安防護能力，同時建構通傳網路資通安全分析與管理平臺，期有效降低通訊傳播網路資安風險，打造數位國家所需之資安基礎建設，推動重點工作，包含建構通訊傳播事業關鍵基礎設施資安聯防體系及完備通訊傳播事業關鍵基礎設施資安防護機制。

肆、人力配置及經費需求(B004&B005)

人力需求及配置表(B004)

一、經濟部

單位：人/年

計畫名稱	107 年度							108 年度	109 年度
	總人力	職級						總人力	總人力
		研究員級(含)以上	副研究員級	助理研究員級	研究助理級	技術人員	其他		
一、建置關鍵基礎設施安全防護計畫(水資源)	0.6	0.3	0.3					0.6	0.6
二、經濟部關鍵資訊基礎設施資安資訊分享與分析平台計畫	0.7	0.1	0.3	0.3				0.7	0.7

二、國發會

單位：人/年

計畫名稱	107 年度							108 年度	109 年度
	總人力	職級						總人力	總人力
		研究員級(含)以上	副研究員級	助理研究員級	研究助理級	技術人員	其他		
107 年度[加速政府資安防護建設計畫]政府骨幹網路資安防護擴充計畫	4	1	1			2		4	4

三、通傳會

單位：人/年

計畫名稱	107 年度		108 年度	109 年度
	總人力	職級	總人力	總人力

		研究員級(含)以上	副研究員級	助理研究員級	研究助理級	技術人員	其他		
數位匯流資通安全分析管理平臺建置與服務	7	3	3	1				7	7

經費需求表(B005)

一、經濟部

單位：千元

計畫名稱	計畫目標	計畫性質	107 年度							108 年度			109 年度		
			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
				人事費	材料費	其他費用	土地建築	儀器設備	其他費用						
一、建置關鍵基礎設施安全防護計畫(水資源)	建構國家資安聯防體系	其他	40,000						40,000	40,000		40,000	40,000		40,000
二、經濟部關鍵資訊基礎設施資安資訊分享與分析平台計畫	建構國家資安聯防體系	其他	15,000						15,000	20,000		20,000	20,000		20,000

二、國發會

單位：千元

計畫名稱	計畫目標	計畫性質	107 年度							108 年度			109 年度		
			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
				人事費	材料費	其他費用	土地建築	儀器設備	其他費用						

107 年度[加速政府資安防護建設計畫]政府骨幹網路資安防護擴充計畫		環境建構與改善	85,000						85,000	80,000		80,000	80,000		80,000

三、通傳會

單位：千元

計畫名稱	計畫目標	計畫性質	107 年度							108 年度			109 年度		
			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
				人事費	材料費	其他費用	土地建築	儀器設備	其他費用						
數位匯流資通安全分析管理平臺建置與服務	建構通傳業者資安聯防體系	其他	60,000						60,000	60,000		60,000	60,000		60,000

四、總經費編列說明

計畫名稱	經費分編	年度				合計
		106	107	108	109	
強化國家資安基礎建設計畫	經濟部	0	55,000	60,000	60,000	175,000
	國發會	0	85,000	80,000	80,000	245,000
	通傳會	0	60,000	60,000	60,000	180,000
總計		0	200,000	200,000	200,000	600,000

伍、 儀器設備需求(B006& B007)

申請機關： (單位：新臺幣千元)

編號	儀器名稱	使用單位	數量	單價	總價	優先順序		
						1	2	3
	無							

申購單價新臺幣 500 萬元以上科學儀器送審表(B007)

申請機關(構)	無				
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：_____) □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 □其他儀器 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(其他儀器專用)

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：500 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，其他儀器原則對外開放，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。

□其他，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	伏度～ 伏度	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：_____

陸、主要績效指標(KPI)

特別預算 6 億元所預期產出之績效指標如下：

年度	106	107	108	109
績效指標	量化指標(%)			
完成關鍵資訊基礎設施領域(經濟部、通傳會等)之資安資訊分享及分析中心(ISAC)建置作業	0	100	0	0
完成關鍵資訊基礎設施領域(經濟部、通傳會等)之資安通報應變中心(CERT) 建置作業	0	50	100	0
完成關鍵資訊基礎設施領域(經濟部、通傳會、國發會等)之資安監控中心(SOC) 建置作業	0	0	50	100

柒、各部會分項計畫

附件 1：經濟部

附件 2：國發會

附件 3：通傳會

附件 1

前瞻基礎建設－數位建設

強化國家資安基礎建設之分項計畫

經濟部

106 年 7 月

壹、計畫緣起

關鍵基礎建設(Critical Infrastructure, CI)，是一個國家為了維持民生、經濟與政府等相關運作而提供之基本設施與服務，包括實體及以資訊電子為基礎之系統，為重要社會基礎功能所需之基礎建設。諸如：公民營電信、電力、能源、金融、醫療、交通、緊急救助等。各種關鍵基礎建設系統，只要牽涉到設備連網，加上採用開放技術架構，都會讓關鍵基礎設施面臨資安風險，相關單位應透過各種資訊分享方式，做到資安事件的提前預警。

由於許多關鍵基礎建設的系統監控和資料擷取系統(以下簡稱 SCADA)有遠端操控系統需求，採用開放的連網架構，國外也陸續傳出各式針對工業控制系統的資安威脅與攻擊事件。依據美國國土安全部(DHS)所屬的工業控制系統緊急應變小組(Industrial Control Systems Cyber Emergency Response Team, ICS-CERT)針對美國包括石油、水力設施、電廠等關鍵基礎建設統計，光是 2013 年遭到外部駭客攻擊的次數就高達 257 次，且其中就有一半的攻擊事件是鎖定能源設施；在 2015 年 ICS-CERT 總共處理 295 個事件通報，其中有 97 個是來自於關鍵基礎建設的事件通報，能源設施有 46 個事件通報，水和污水系統設施則有 25 個事件通報。ICS-CERT 所處理的系統弱點協調工作件數，近年來也有增加的趨勢，從 2014 年的 231 件，2015 年為 486 件，增加幅度為 2 倍多。

鑒於本部主管的能源與水資源關鍵基礎設施之數位化工業控制系統資通安全需求，在「資安即國安」的國家政策方針下，依據「數位國家・創新經濟發展方案」及「第五期國家資通安全發展方案 (106 至 109 年) 」草案策略，規劃「打造安全可信賴的數位經濟時代」及「建置國家資安機制，提升自我防護能量」，經濟部擬定「經濟部關鍵基礎設施安全防護計畫」，強化水資源關鍵基礎設施之安全，開發建置經濟部關鍵資訊基礎設施(Critical Information Infrastructure,CII)資安資訊分享與分析平台 (Economic CII Information Sharing and Analysis Center，以下簡稱 E-ISAC)，並透過國家資安情資分享中心(N-ISAC)與其他領域 ISAC 平台串接，以建立跨領域聯防機制，為關鍵資訊基礎建設之整體資安防護奠定基礎，提升能源與水資源領域關鍵基礎設施之資通安全。

貳、計畫目標

目標說明

強化水資源關鍵基礎設施資安防護，防範水資源關鍵資訊基礎設施免於遭受資安攻擊之風險，提升水資源關鍵基礎設施提供機關資訊基礎環境之安全性及穩定性。透過建置 E-ISAC 平台建立關鍵資訊基礎設施資安聯防機制，為整體關

鍵基礎建設施之資安防護奠定基礎，降低資通安全風險對關鍵基礎設施運作之影響。

執行策略及方法

分項一：建置關鍵基礎設施安全防護計畫(水資源)

計畫架構

水利署於 106 年度建置「水資源資安資訊分享與分析平台」(W-ISAC)之初步架構與應用系統。於本計畫，將持續擴充「水資源資安資訊分享與分析平台」之功能與軟硬體設備，其相關軟硬資訊設備將研擬於經濟部水利署與新北市政府聯合新建的安坑輕軌捷運 K8 站(本工程列入前瞻基礎建設-軌道交通建設之一)水利大樓資訊機房佈建，增列建置二線資安監控中心(Security Operation Center)強化資安事故發現能力，逐步監控水庫水資源領域相關產業鏈並提供監控及情資分享。除前述針對資訊安全面之強化外；另外，依專家建議盤點使用之相關水工機械及電控使用之設備將參酌 SIL(Safety Integrity Level)安全完整性標準，俾後續評估其設備進行智慧管理化的可行性。

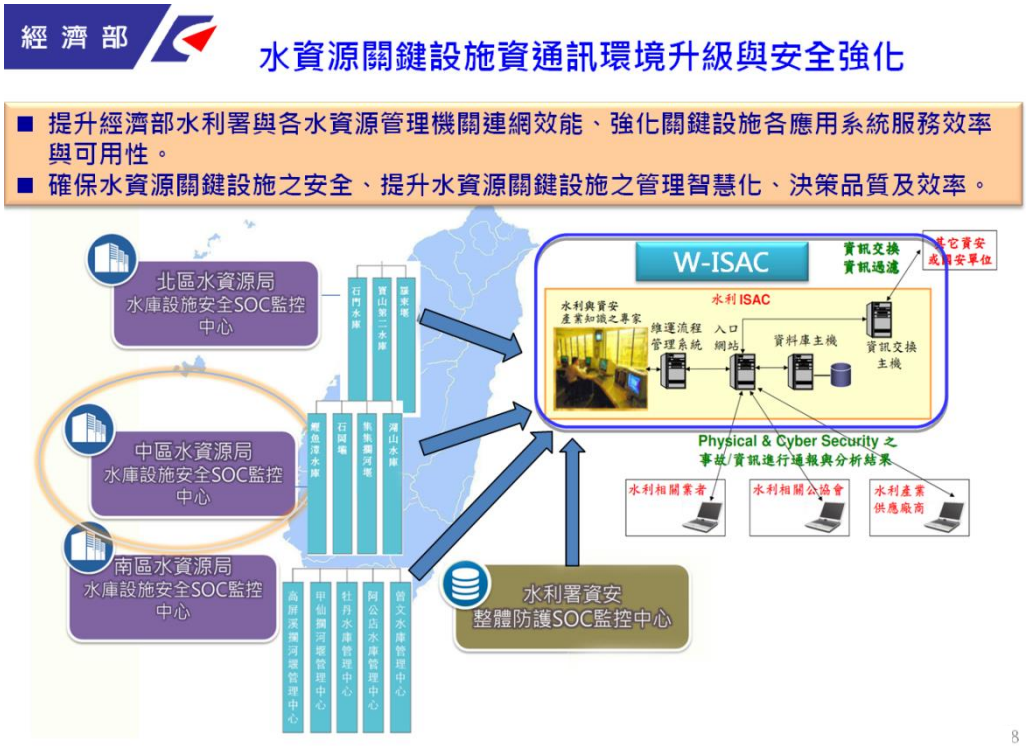


圖 1 水資源關鍵基礎設施資通訊環境架構圖

計畫說明

本計畫主要是推動水資源產業所屬關鍵資訊基礎設施之防護規劃，藉由上述架構，主要工作包括(一)強化水資源關鍵資訊基礎設施資安防護能力及(二)辦理 ISAC 資料交換規劃與 CERT 資料擷取平台建置所需經費軟硬體資訊設備。

強化水資源關鍵基礎設施資安防護能力

水利署及所屬現有水資源關鍵基礎設施機房配置升級及實體安全管控的強化，諸如：機房配置綠色節能、智慧管控等議題不斷推陳出新，而實體安全以機房環境及硬體設備管理為重點，包含有「高效能源管理」、「建置虛擬化基礎平台」，以及「強化安全管控」等，工欲善其事，必先利其器。此外，現有之入侵防禦系統(IPS)、防火牆等安全產品皆屬傳統分層防禦策略中的基本元件，其用途是解決安全問題，當水利署面對經常發生之新型態網路阻斷服務攻擊(DDoS)，此類設備無法解決 DDoS 攻擊的根本問題—網路可用性，爰規劃並建置能強化水利署資安防護之新型態的安全解決方案。

另外，經濟部水利署現有關鍵資訊基礎設施之端點防護機制並未涵蓋行動裝置範疇，鑒於技術變遷行動裝置已達到廣泛使用之境，行動裝置透過網際網路連線即可達成資料收發瀏覽、網頁瀏覽與管理，若行動裝置未妥善防護將造成整體資訊安全防護之缺口，故將規劃行動裝置防護納入整體資訊設備端點防護之一環。

工作項目

1. 規劃升級機房配置及強化實體安全管控並建置 W-ISAC 監控儀表版、骨幹多層次網路防護機制。
2. 規劃並建置分散式阻斷主動攻擊分析、偵測與防禦機制。
3. 規劃並建置雲端智能分析與預警及阻止新興的僵屍網路和應用層攻擊機制。
4. 規劃並建置自動化攻擊減緩機制。
5. 規劃並建置滲透攻擊防護、網頁過濾防護服務及行動裝置安全防護機制，使行動裝置具備網頁過濾防護與隔絕有害程式碼之侵犯。
6. 規劃並建置行動裝置資料防護機制，將行動裝置上之資料加密保護，並可透過遠端操做鎖定及清除資料，以保護重要機敏資料。

水資源領域 ISAC 資料交換規劃與 CERT 資料擷取平台建置

經濟部水利署目前正研擬「水資源資安資訊分享與分析平台」(W-ISAC)之初步架構與應用系統。於本計畫將執行水資源領域 ISAC 資料交換規劃與 CERT 資料擷取平台建置，包含相關軟硬體資訊設備的構建。此外，為提升水利署網路閘道網路流量的有效監控，以快速偵測並回應鎖定目標攻擊與進階威脅，擬規劃建置水利署進階網路威脅防護平台。此平台規劃具有本地與雲端偵測及模擬分析技術之能力，能快速發掘並分析水利署網路中之惡意程式、C&C 通訊連線，以及現行防護無法偵測到的隱匿攻擊，並加以有效阻擋。

工作項目

1. 整合水利署暨所屬機關現有資安防護產品訊息，以提供平台資安情報共享與即時分析。

2. 規劃水資源關鍵基礎設施 SCADA 入侵偵測研究，及規劃建置符合水利署客製化需求之惡意程式、C&C 通訊、駭客活動偵測引擎、交叉關聯分析以及模擬分析元件。
3. 規劃並建置攻擊來源調查、分析與阻擋元件。

分項二：經濟部關鍵資訊基礎設施資安資訊分享與分析平台計畫

計畫架構

本計畫主要是強化經濟部轄管之水資源及能源關鍵資訊基礎設施之防護規劃，藉由營運 E-ISAC 平台，與所屬機關(構)單位及國家層級 ISAC(N-ISAC)合作介接進行情資交換，強化整體水資源及能源資安防禦與應變措施，全程計畫規劃架構如下圖所示：

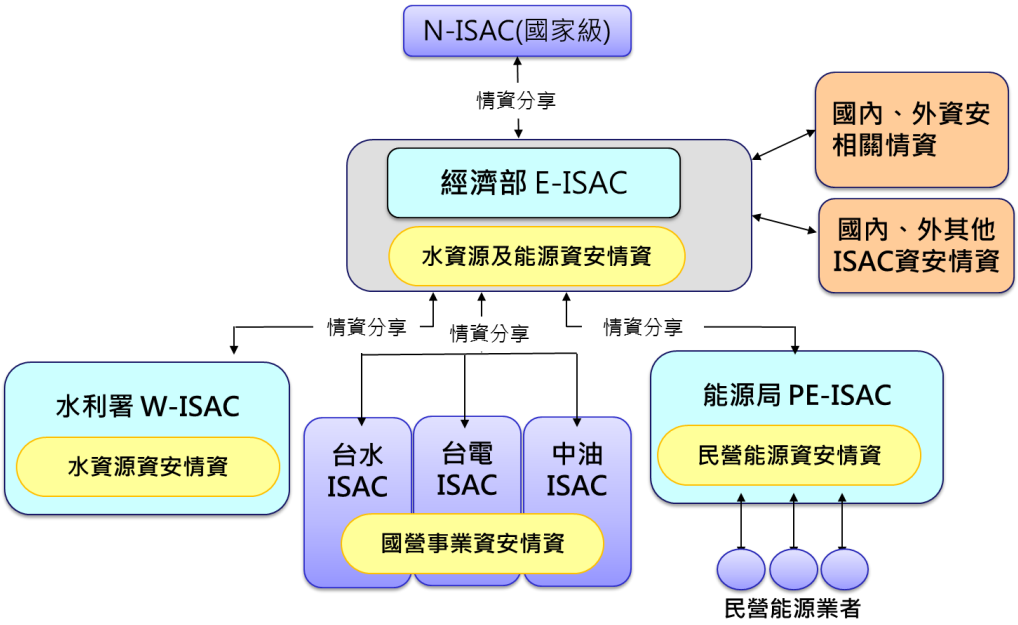


圖 2：經濟部關鍵資訊基礎設施資安情資交換及分享整體架構

計畫說明

經濟部關鍵資訊基礎設施資安資訊分享與分析平台(以下簡稱 E-ISAC)開發建置

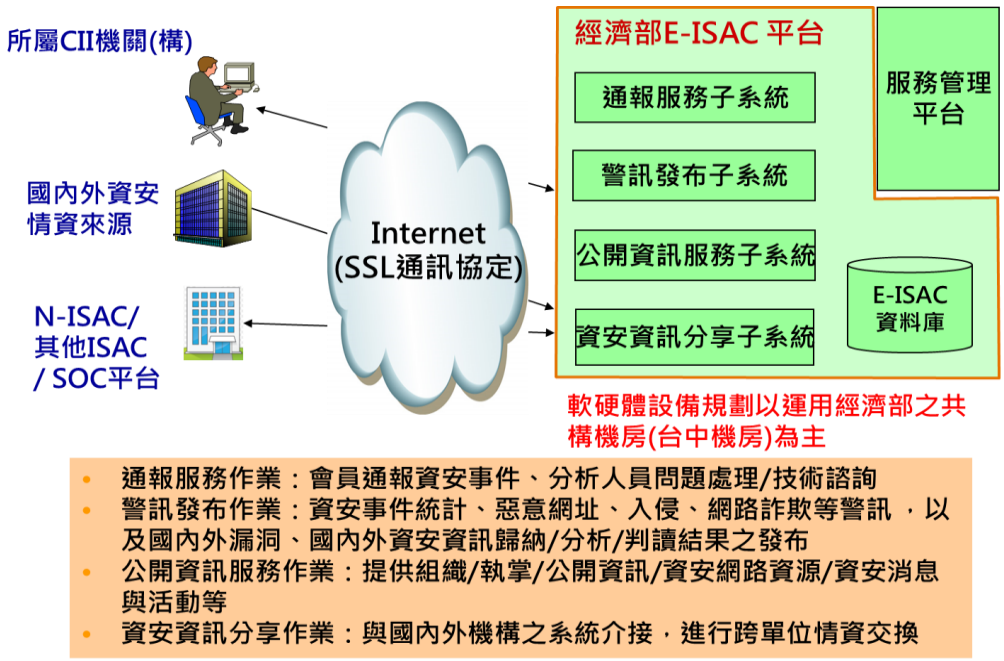


圖 3：經濟部關鍵資訊基礎設施資安資訊分享與分析平台功能架構

系統擬訂主要功能概述如下：

通報服務子系統

本子系統為本平台之前端資安事件資料來源，提供經濟部所屬水資源及能源轄管機關(構)進行資訊安全事件通報。功能包括資安事件通報新增、修改、查詢與結案及資安事件通報審核機制等。

警訊發布子系統

本子系統提供本平台維運人員將資安相關預警警訊與防範措施，發布給經濟部所屬相關機關(構)會員(介接平台)，其功能包括警訊新增、修改與刪除；警訊查詢、審核、發布與退件；及警訊回覆處理、彙整及狀態追蹤等功能。

公開資訊服務子系統

本子系統提供經濟部所屬相關機關(構)會員取得本平台之公開說明資訊、資安相關網路資源、資安消息與活動的主要管道。其功能包括：最新消息、近期活動、本平台簡介及威脅情報與專欄文章公告功能。

資安資訊分享子系統

本子系統為與國內 N-ISAC 進行跨單位資安情資交換。資料交換將 STIX 格式之標準結構化語言，以描述網路威脅、資安事件及應變措施等情報資訊，資安情報交換機制則透過 TAXII 交換傳輸機制，以自動化接收與對外傳送各式資安情報資訊。使用者可利用本系統之網站介面手動交換資訊，亦可藉由系統間之 TAXII API 進行資訊之自動交換。其功能包括：資安事件交換機制及資安情資編

輯。

強化 E-ISAC 之資通安全防護

由於本平台所提供之情資非屬公開資訊，為避免資訊被未授權揭露或取得，需強化平台所在基礎環境及平台本身之機密性、完整性及可用性之資通安全防護。因此除於平台開發建置階段及功能設計時須有安全性考量，另於平台開發完成後須進行原始碼檢測、弱點掃描及滲透測試等，使得上線，再配合於平台運作基礎環境引進相關防護機制，強化縱深防護，使得所有相互界接之平台，不會因資通安全事故而相互干擾及影響。

E-ISAC 作業管理制度建置

為能落實 E-ISAC 之營運及處理能力，本計畫將建置相關管理制度與程序文件，如資安資訊分享與分析平台規劃與運作規範、組織章程與運作機制、緊急應變處理程序書等，以提升整體效能。

E-ISAC 平台維運管理

本平台之各項維運作業分述如下：

通報服務作業

在資訊安全越趨重要的網際網路環境，資安事件的即時通報對於資安事件的儘速解決為一重要的工作，若產生資安事件，即時通報回覆為處理問題的第一步。當經濟部所屬相關機關(構)會員發生資安事件，可立即透過本平台系統進行資安事件通報，本平台人員於接獲通報後需即時取得通報資訊，將進行進一步的問題處理、或轉介技術諮詢。

警訊發布作業

本平台規劃提供有關資安事件統計、惡意網址、入侵事件、網路詐欺等資安威脅警訊與防護措施建議等資訊給經濟部所屬相關機關(構)會員(介接平台)。
本平台維運人員將主動蒐集國內外漏洞通告並整理國內外資安相關訊息加以歸納、分析、判讀，並針對可能造成危害的重大威脅，提早發出警訊，以供經濟部所屬相關機關(構)會員(介接平台)早期進行防禦減低傷害及損失。

公開資訊服務作業

本子系統目的在於提供會員了解本系統之組織架構、執掌、功能，及本系統之公開說明資訊、資安相關網路資源、資安消息與活動的主要管道。

資安資訊分享作業

本平台與國內其他資訊安全資訊分析分享機構之系統平台介接，進行跨單位的資安情資交換，例如 N-ISAC，透過自動化或手動方式提供經濟部所屬相關機關(構)會員(介接平台)。

規劃 E-ISAC 與經濟部關鍵基礎設施提供單位 ISAC 及 N-ISAC 介接介面

參考 N-ISAC 訂定之 STIX 格式之標準結構化語言及 TAXII 交換傳輸機制，研擬 E-ISAC 和下一階層各關鍵基礎設施提供單位(台電、台水、中油、能源局及水利署等)ISAC 之資訊交換介面規格，以及上一階層 N-ISAC、國內外其他領域 ISAC 之資訊交換介面規格。

經濟部關鍵資訊基礎設施威脅燈號研究

水資源及能源領域威脅燈號研究需涵蓋實體安全、人員安全、資通安全、資安事故等面向及其評分準則，設計燈號計算之理論、各面向之權重與演算法，依據前述定義及準則蒐集相關風險資訊與資安資訊，進而計算並簡潔的顯示資安現況水準。

本計畫綜合蒐集各關鍵基礎設施提供單位(台電、台水、中油、能源局及水利署等)ISAC 之威脅燈號，研究分析後制定經濟部整體關鍵資訊基礎設施之威脅燈號。

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。

SWOT 分析表

SWOT 分析	
優勢(Strength)	劣勢(Weakness)
國內 SOC 業者在 IT 領域的情資、日誌收集與分析技術成熟，藉由該經驗，進入 OT(Operational Technology)領域的情資、日誌收集與分析，更有脈絡可依循。 經濟部國營事業委員會於 97 及 98 年曾經執行資安資訊分享與分析專案，針對油、電、水領域之資安情資進行蒐集、分享，已有建立相關系統與推廣之經驗。 行政院目前已擬具「資通安全管理法」草案，相關資安管理規範後續將有法源依據，關鍵基礎設施提供者亦須符合法律的要求，對推動能源領域資安資訊分享將有正面幫助。	關鍵基礎設施提供者，可能認為分享資安情資會導致營業機密外洩，影響營運績效，導致不願分享相關情資。 工業控制系統之入侵偵測與分析等，目前資安業界具備相關能力者甚少，相關技術仍屬萌芽期，已具成熟度的工具亦不多，較難以藉由此種方式獲得情資。
機會(Opportunity)	威脅(Threat)

經濟部轄管水資源及能源領域，藉由此計畫可分享資安相關事故與資訊，全面提升能源領域之資安水準，有助於關鍵資訊基礎建設之整體資安防護。 透過該平台向下與本部所屬水利署、能源局與台電公司、中油公司及台水公司之資安資訊分享與分析平台進行情資交換，以強化資安防護訊息之即時性與有效性，並向上透過國家資安情資分享中心與其他領域資安資訊分享與分析平台串接，以建立跨領域聯防機制。	關鍵基礎設施之工業控制系統攻擊的技術日新月異，而關鍵資訊基礎建設保護的情資不足，如遇到攻擊可能造成威脅。 駭客藉由入侵資安資訊分享與分析平台，盜取相關情資。

SWOT 矩陣分析

SWOT 矩陣分析		內部分析	
		優勢(S)	劣勢(W)
外部分析	機會(O)	SO 策略(Max-Max) 篩選出國內具有研發能力、資安管理經驗豐富的 SOC 業者參與，蒐集水資源及能源營運紀錄資料並進行分析，提升工業控制系統入侵偵測之分析及處理能力，發展符合國內環境的資安事故之處理規則。 善用經濟部國營事業委員會過去建置油、電、水國營事業 ISAC 之執行經驗，當可建置更為完備、更具成效之 E-ISAC 平台。 「資通安全管理法」之通過將更有利關鍵資訊基礎設施資安防護之推動。	WO 策略(Min-Max) 透過制訂 E-ISAC 組織章程與運作機制、緊急應變處理程序等，建立與經濟部轄管水資源及能源領域 ISAC 之通報及分享管道，使資安情資能充分流通，達到聯防的效果。 透過蒐集經濟部轄管水資源及能源領域 ISAC 之情資通報交換，進行分析處理後將相關資訊分享於相關機關構，提升整體資安防護能力。 本部技術處及工業局主導技術研發及產業推廣，透過相互合作，找出解決目前面臨之工業控制系統之入侵偵測與分析等問題及需求之解決方案。 引進 SCADA 之入侵偵測產品，整合 SOC 與此類產品，蒐集水資源廠區的營運紀錄資料。
	威	ST 策略(Max-Min)	WT 策略(Min-Min)

	脅 (T)	藉由經濟部建立 E-ISAC 下一階層與轄管水資源及能源領域 ISAC 介接，上一階層與 N-ISAC 界接，形成完整之三層式聯防體系。 經濟部所屬之中油、台電及台水等國營事業擁有豐富的關鍵資訊基礎設施資訊，藉由 E-ISAC 之建立將可提供相關訊息，以培養關鍵資訊基礎設施工業控制入侵防禦之能量。	透過 E-ISAC 與國內外資安組織進行情資分享，以蒐集關鍵資訊基礎設施遭受攻擊之最新事件及攻擊技術，及早研擬預防措施。 透強化安資訊分享與分析平台所在基礎環境之資通安全，並且運用二階段認證機制、原始碼檢測、弱點掃描及滲透測試等，強化平台本身資通安全。 尋找適合水資源廠區標的進行 SCADA 測試與分析，確認此類系統搭配適當之偵測規則確有能力及早發現廠區。

目標實現時間規劃

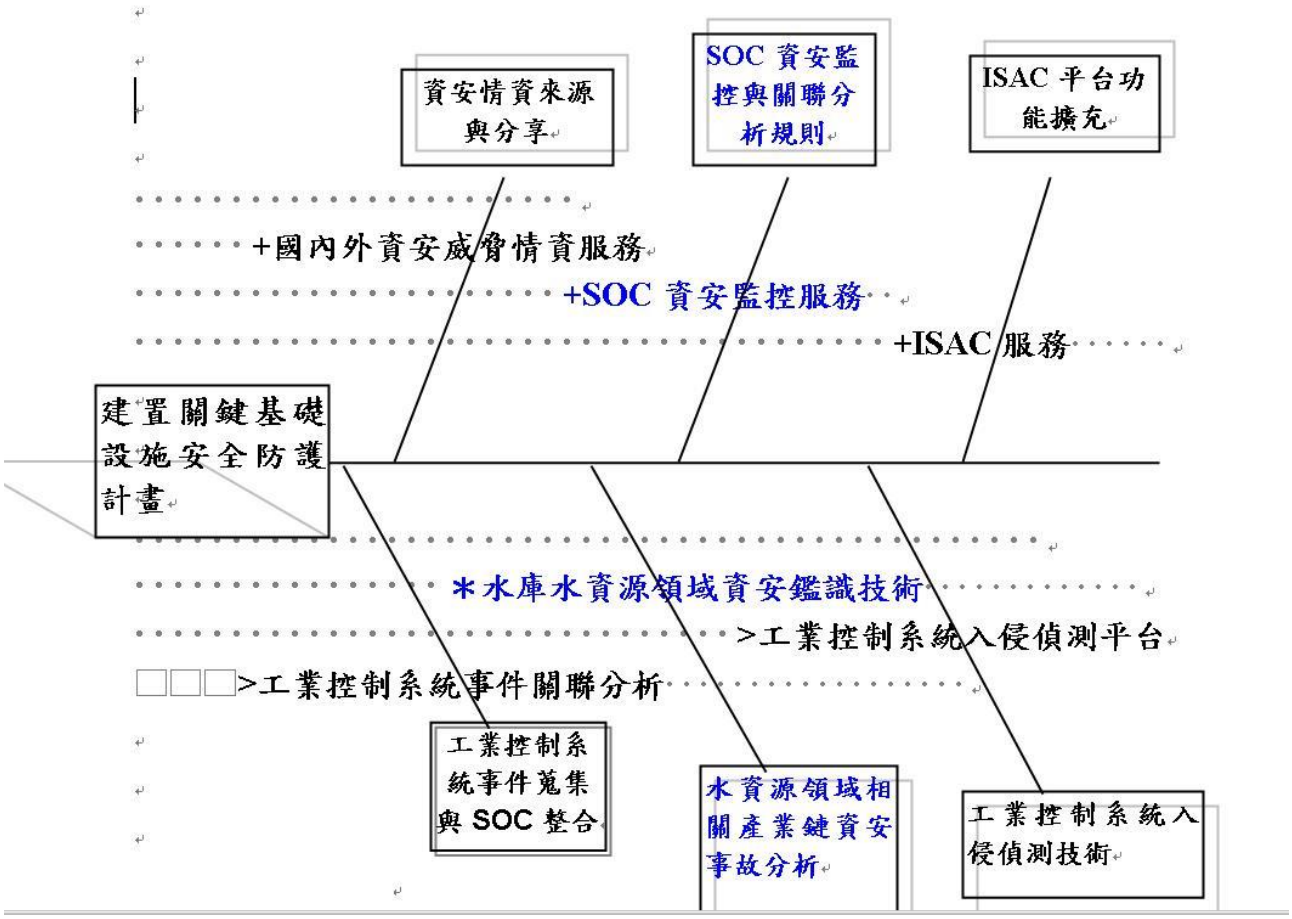
分項目標	執行年度	細部工作名稱	執行策略說明(請依細部、子項計畫逐層說明)
建置關鍵基礎設施安全防護計畫(水資源)	107	強化水資源關鍵基礎設施資安防護能力	規劃並建置 W-ISAC 監控儀表版、骨幹多層次網路防護機制。 規劃並建置分散式阻斷主動攻擊分析、偵測與防禦機制 規劃並建置雲端智能分析與預警及阻止新興的僵屍網路和應用層攻擊機制 規劃並建置自動化攻擊減緩機制 規劃並建置滲透攻擊防護、網頁過濾防護及行動裝置安全防護機制。 規劃並建置行動裝置管理平台。
	107	ISAC 資料交換規劃與 CERT 資料擷取平台建置	整合水利署暨所屬機關現有資安防護產品訊息，以提供平台資安情報共享與即時分析。 規劃水資源關鍵基礎設施 SCADA 入侵偵測研究，建置符合本署客製化需求之惡意程式、C&C 通訊、駭客活動偵測引擎、交叉關聯分析以及模擬分析元件。 規劃並建置攻擊來源調查、分析與阻擋元件。
建立經濟部關鍵資訊基礎建設資安資訊分享與分析平台(E-ISAC)	107	E-ISAC 開發建置	E-ISAC 初步規劃與基本功能開發 E-ISAC 基本環境建置
	107	E-ISAC 作業管理制度建置	E-ISAC 作業管理制度研擬與規劃 E-ISAC 作業管理制度環境建置
	107	E-ISAC 維運管理	E-ISAC 資安資訊分享管理、通報事件管理、事件追蹤與維運流程檢視的管理工作 收集關鍵資訊基礎建設之資訊安全趨勢與國際 ISAC 資訊，並依據本部現況與國內環境，精進並強化 E-ISAC 平台功能、流程
	107	建置與經濟部關鍵基礎設施提供單位 ISAC 及 N-ISAC 介接介面	參考 N-ISAC 訂定之 STIX 格式之標準結構化語言及 TAXII 交換傳輸機制，規劃與與經濟部關鍵基礎設施提供單位 ISAC 及 N-ISAC 介接介面。

分項目標	執　行年度	細部工作名稱	執行策略說明(請依細部、子項計畫逐層說明)
	107	建置經濟部關鍵資訊基礎設施威脅燈號	綜合蒐集各關鍵基礎設施提供單位(台電、台水、中油、能源局及水利署等)ISAC 之威脅燈號，研究分析後制定經濟部整體關鍵資訊基礎設施之威脅燈號。

重要科技關聯圖例

分項一：建置關鍵基礎設施安全防護計畫(水資源)

重要科技關聯圖例



(註) 科技成熟度之標註：

＋：我國已有之產品或技術

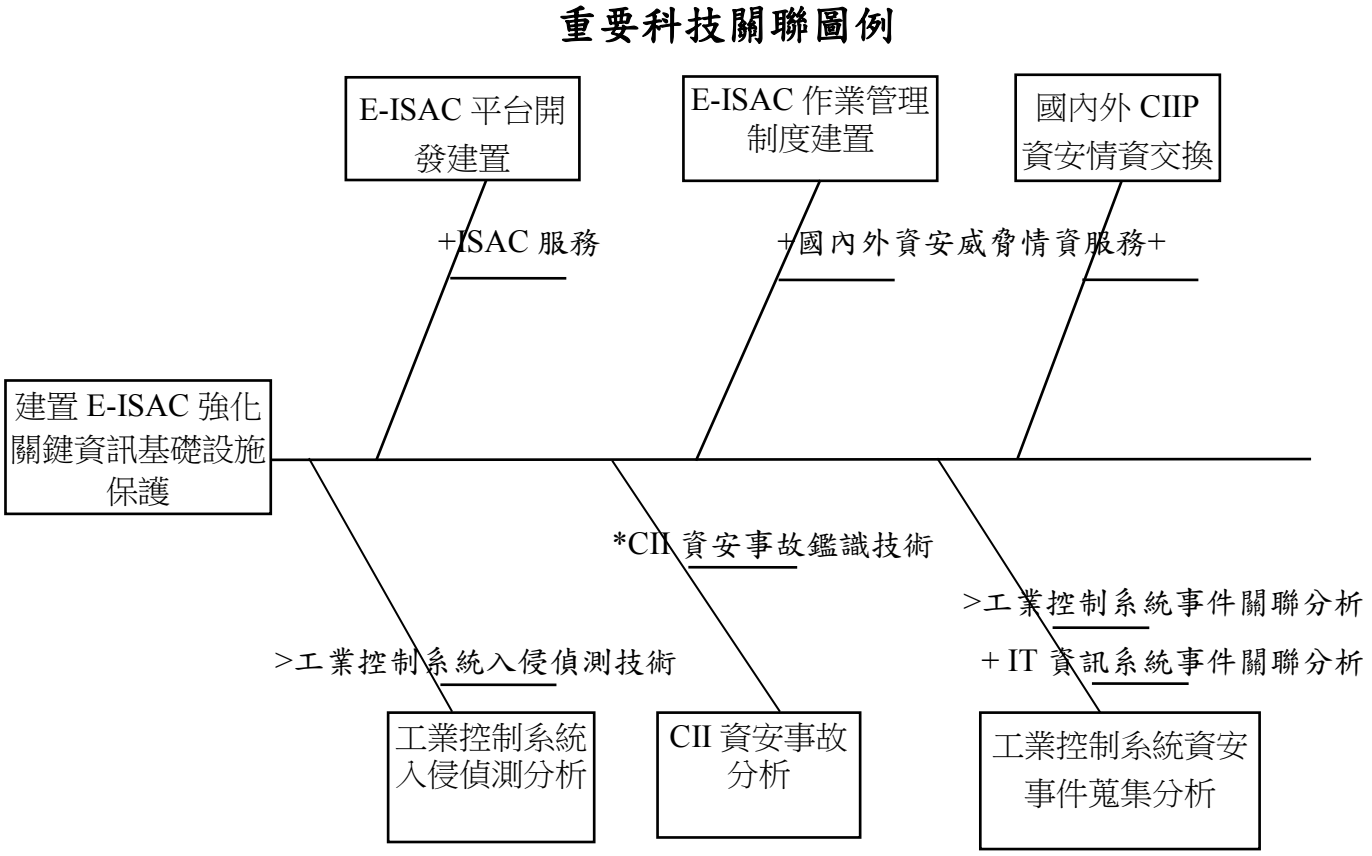
＊：我國正發展中之產品或技術

＞：我國尚未發展中產品或技術

產品或技術若與「智慧財產權」有關亦請加註說明

分項二：經濟部關鍵資訊基礎設施資安資訊分享與分析平台計畫

重要科技關聯圖例



(註) 科技成熟度之標註：

＋：我國已有之產品或技術

＊：我國正發展中之產品或技術

＞：我國尚未發展中產品或技術

產品或技術若與「智慧財產權」有關亦請加註說明

參、預期效益、主要績效指標(KPI)及目標值

目標	預算	預期成果效益	績效指標	評估方法	目標值訂定之依據
建置關鍵基礎設施安全防護計畫(水資源)	40,000(千元)	強化經濟部水利署及所屬相關設施之安全。	1.完成水資源關鍵基礎設施機房配置及實體安全管控、骨幹多層次網路防護機制。 2.完成資料交換規劃與資料擷取平台建置所需經費軟硬體資訊設備。 3.完成滲透攻擊防護及網頁過濾防護服務。	數據統計	
建立經濟部關鍵資訊基礎建設資安資訊分享與分析平台(E-ISAC)	15,000(千元)	強化關鍵資訊基礎設施保護，建立經濟部及所屬機關構關鍵資訊基礎設施資安聯防制度。	1. 完成 E-ISAC 平台建置。 2. 完成 E-ISAC 作業管理制度建置。 3.完成與經濟部關鍵基礎設施提供單位 ISAC 及 N-ISAC 介接介面設計。 4.完成經濟部關鍵資訊基礎設施威脅燈號研究。	數據統計	

附件 2

前瞻基礎建設－數位建設

強化國家資安基礎建設之分項計畫

國發會

106 年 7 月

壹、計畫緣起

一、政策依據：

行政院國家資通安全會報設置要點：依據行政院國家資通安全會報設置要點，本會編組於「網際防護體系」「政府資通安全組」「電子化政府分組」，主要負責政府骨幹網路安全相關事宜。

國家關鍵基礎建設防護指導綱要：行政院於 103 年 12 月函頒修正之「國家關鍵基礎設施安全防護計畫指導綱要」，本會負責關鍵基設施之重要元件設施為政府網際服務網(GSN)骨幹網路、政府共構機房，其中 GSN 骨幹網路經行政院核定為一級關鍵基礎設施。

二、擬解決問題之釐清：

行政院於 104 年 8 月訂頒「行政院及所屬機關資安分級作業要點」，律定各級(A、B、C)機關之資安要求及防護縱深機制，以防範潛在資安威脅，進而提升國家資安防護水準，本會主責政府骨幹網路安全，配合行政院資安政策，於政府骨幹網路部署資安強化措施，以確保 GSN 骨幹網路傳輸效能、穩定性及安全性。

三、目前環境需求分析與未來環境預測說明：

1. 分散式服務阻斷攻擊(DDoS)趨勢升高

在 Radware 2011 全球應用程式及網路安全報告(Radware’s 2011 Global Application and Network Security Report)中顯示，網際網路接取業者(ISP)及政府機關遭遇 DDoS 攻擊的危險性大幅增加，分別落在中度及高度被攻擊風險區域；在賽門鐵克發佈的安全鑑識報告中，對於國家與民族意識的問題，網路駭客集團也不吝於表示其主張，以挖掘機密資訊使其曝光、攻擊主要政府網站及設施做為手段，迫使國家及特定企業有所改變 。

102 年 5 月廣大興 28 號事件，在臺菲雙方由政治議題擴展到了民間藉由網路互相攻擊的狀況；去(103)年蘋果日報因為反對中國高壓治理香港的立場，先後遭到多次 DDoS 攻擊而網站癱瘓；今(104)年 8 月教育部新舊課綱爭議，造成總統府、教育部及眾多部會網站遭受國際駭客組織匿名者攻擊等；GSN 做為政府機關骨幹網路資安的守門員，未來所需面對 DDoS 的風險不言可喻，如何在資源有限的情況下確保政府骨幹以及各級機關的安全及網路正常運作，並在阻擋攻擊後彙整相關攻擊軌跡證據及報表等，作為後續防護增強改善，以達到有效防阻有心的網路攻擊者，是現階段 GSN 網路的重要工作。

2. 持續攻擊或置換網站首頁

根據賽門鐵克 2014 年網路安全威脅研究報告指出，2013 年網頁攻擊次數較 2012 年成長 23%，顯示網站仍然是駭客的主要目標之一，政府網站通常是政府機關提供為民服務的入口，亦是民眾獲取政府資訊的重要管道，網路駭客則利用

系統漏洞、隱碼攻擊、社交工程等手法，設法滲入機關網站植入惡意程式，或在網頁中埋下惡意連結，伺機對瀏覽網頁者植入惡意程式，達到控制電腦及展現其成果之目的。此種攻擊手法不僅可能造成機關重要資訊外洩風險，後續也可能被駭客作為 DDoS 攻擊的跳板，尤其是機關網頁如被置換，對機關形象聲譽更造成重大影響。

3. 政府部門是 APT 攻擊鎖定的對象

韓國在 2013 年 3 月遭受國家級 APT 攻擊，駭客潛伏 8 個月入侵上千次，發動攻擊時造成 6 家企業，超過 48,700 臺電腦、伺服器與 ATM 伺服器接連當機，硬碟開機磁區損毀，無法重新提供服務，數千臺 ATM 故障，網路銀行與信用卡服務也受創；而國內過去發生公文電子交換網路系統遭駭客長期埋伏，以有組織、有系統地入侵，從國際資安攻擊事件及各項調查顯示，2014 年台灣被攻擊裝置最多的地區排名在前 20 名，若以 APT 幕後操縱伺服器數量分佈來看，台灣亦排名前 15 名以內，因此不論被攻擊的裝置數量或是幕後操縱的伺服器，顯示台灣都是 APT 攻擊的主要地區之一，GSN 如何協助防範 APT 攻擊亦是現階段重點防護之一。

四、計畫定位：

本會(原行政院研考會)自民國 86 年起規劃建置「政府網際服務網」（Government Service Network，簡稱 GSN），建構以網際網路為基礎之全國骨幹網路，提供各級政府機關接取之總線路達 3 萬多路，形成政府機關整體性網路環境，廣泛應用於中央及地方各級機關上網、村里巷口監視器、河川土石、公文交換等；為強化政府骨幹網路整體資安防護，於骨幹網路提供入侵防禦、垃圾郵件過濾、網頁瀏覽安全及小流量之分散式服務阻斷攻擊(DDoS)防護等資安防護機制。

鑑於各機關正積極發展巨量資料、雲端服務、開放資料、智慧城市等重大科技施政方向，為提供各機關穩定、高品質及安全的網路環境，爰透過政府骨幹網路防護作為整體資安防禦，並輔以各部會單一目的性的防護，以有效防範政府機關遭受資安攻擊之風險，降低公務員上網之資安危害，提供機關安全穩定的政府網路，發展各項創新為民服務。

貳、計畫目標

一、目標說明：

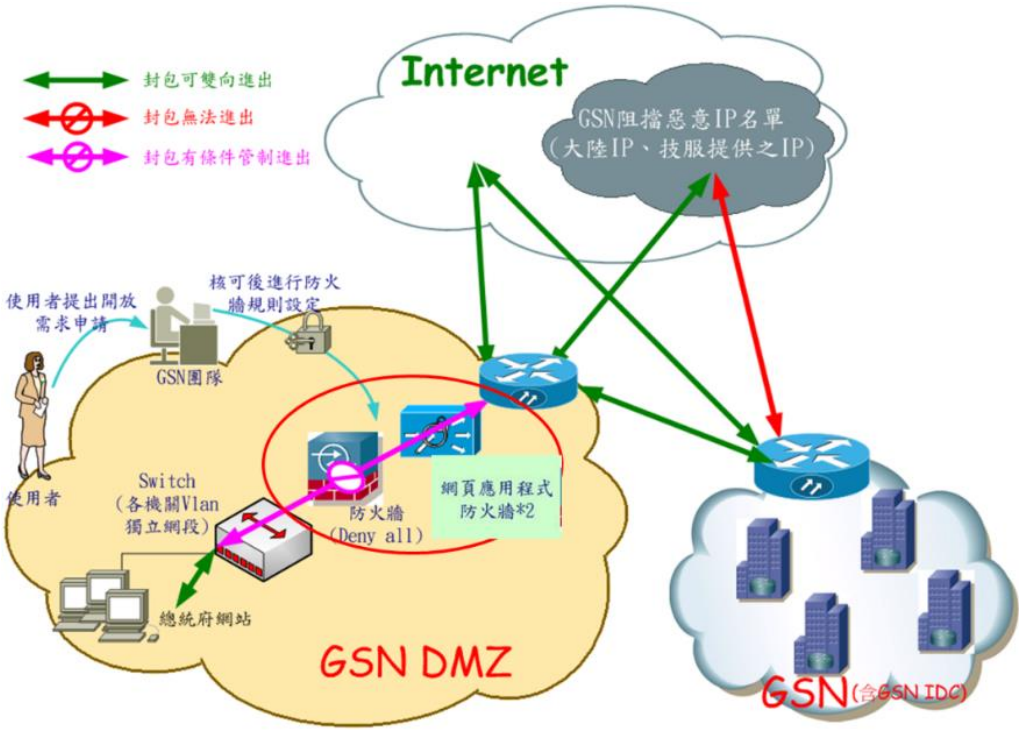
整體規劃並提供政府骨幹網路資訊安全監控防護機制，建立骨幹網路與機關端縱深防護機制，透過事前偵測阻擋惡意訊息或攻擊及事後分析，有效提升政府網路安全，確保政府提供為民服務網站穩定性及可用性，提高民眾滿意度。
透過區域聯防之形式，持續監控分析全球之惡意活動與異常 IP，以最少資源達到聯合防禦的資安防護效果。統一部署及建置共通性資訊安全防禦機制，減少基層機關資安人力及預算不足問題。

二、執行策略及方法

1. 網頁應用防火牆(WAF)防護服務

近年來，不少機關遭受到駭客以各種新型態攻擊，而駭客攻擊手法越來越複雜且頻繁，取得攻擊的工具與管道也越來越容易，而其中有不少攻擊直接針對網站伺服器，使得網頁應用成為資安漏洞的一環，傳統防火牆與入侵防禦系統 (IPS) 等架構並無法抵抗應用程式層級的攻擊，如跨網站攻擊 (Cross-Site Scripting) 以及 SQL Injection 攻擊等，依據 OWASP（Open Web Application Security Project）組織每年公佈資安威脅，網站漏洞仍高居十大威脅之一。

網站資安風險除了程式碼及應用程式本身之漏洞，尤其是服務上線前未依規定先進行程式原始碼檢測，或出現零時差漏洞攻擊，更提高政府機關網站資訊安全風險威脅。本計畫規劃於 GSN 防護專區部署網頁應用防火牆(Web Application Firewall，WAF)服務，配合 GSN 入侵防護服務的防禦廣度，無論是來自網際網路或是 GSN 內部網路之存取，均可進行過濾封包，保護 GSN 防護專區及行政院及所屬委員會雲端資料中心重要網站，以降低網頁遭受篡改、網頁附掛木馬程式等安全事件的發生率，加強網站防護深度，整體服務示意圖如下：



圖：網頁應用防火牆(WAF)防護架構

2. 進階持續性威脅(APT)偵測防護

政府機關網路正面臨日益升高的針對性攻擊威脅攻擊，如 2013 年 5 月初國家檔案管理局之電子公文交換系統遭駭，使得相關單位下載電子公文官網上提供的新版 eClient 更新程式並安裝後到電腦後被駭客控制，攻擊手法之複雜與精密程度是過去所罕見，應該是駭客長期埋伏且是有組織、有系統的行為；韓國也在 2013 年 3 月韓國遭受國家級惡意攻擊，駭客潛伏 8 個月入侵上千次，發動攻

擊時造成 6 家企業，超過 48,700 臺電腦、伺服器與 ATM 伺服器接連當機，硬碟開機磁區損毀，無法重新提供服務，數千臺 ATM 故障，網路銀行與信用卡服務也受創。

這些設計精巧、隱蔽性高、重複性低、具目標性、且攻擊持續的威脅被稱為進階持續性攻擊(APT)，這些攻擊目標明確，危害性強。很多的 APT 攻擊手段都是利用未公開揭露漏洞，製作惡意軟體，或者在合規文件中添加惡意代碼等等，此時傳統依據特徵值檢測、黑名單比對及靜態分析之安全機制幾乎失效。因此須透過其他機制和手段來模擬真實環境，探測未知內容的行為。

因此，本計畫規劃建置政府機關進階持續性威脅(APT)偵測防護服務 APT 資安防護服務，透過特徵比對、行為分析、沙箱模擬等多種分析方式，鎖定 APT 攻擊，於攻擊開始階段立即阻絕，並檢測網頁或電子郵件流量，自動關聯化分析感染事件瞭解攻擊鏈行為，鎖定惡意攻擊感染範圍，快速進行隔離與通報應變，杜絕社交工程手法帶來的潛常攻擊。

3. 深層網路流量分析與安全管理服務

政府網路流量包含各式應用服務，其中包含 P2P、IM、VoIP、Streaming、FTP、SSL、Oracle、Tunnel 等應用程式，網路攻擊行為可能潛藏於其中，透過深層識別封包檢測技術可辨識用戶網路行為，例如異常應用程式使用或異常連線存取行為等。如可辨識某一機關對外使用 tunnel 流量至國外 IP 時，可告警管理者異常行為，確認此網路連線是否正常。同時此服務可針對 IP 或應用程式提供保障頻寬，最大頻寬多少，及其優先順序，政府網路可預先分配網路資源保障特定 IP 或應用服務頻寬，防止 DDoS 攻擊發生時影響其他使用共同電路出口之用戶。

本計畫將提供頻寬管理功能，針對機關申租電路提供流量門檻，避免機關遭受 DDoS 時，其他機關連同遭受影響，提供流量分析服務，查找異常應用程式存取行為，強化網路安全控管。

4. 強化分散式阻斷式攻擊(DDoS)流量安全管制服務

DDoS 攻擊近日快速增加，從多個 IP 位址發送大量要求至各種網路設備或網路資源，迫使線上服務中斷，如 2017 年初證券業的金融勒索一案，但除面對頻寬耗盡的攻擊手法外，還有應用層的資源耗盡型的攻擊，例如快速 TCP 連線、HTTP 慢速攻擊、SSL 連線攻擊、大量 HTTP 請求、DNS NXDomain 攻擊等，非單究透過增加頻寬或是清洗流量方式解決 DDoS 攻擊，應透過混合式防禦手法由 ISP 端進行流量清洗(Clean Pipe)機制，並結合 CPE 端應用層攻擊 DDoS 防禦機制，雙管齊下保護重要系統資源使用。目前政府網路前端已提供流量清洗(Clean Pipe)服務，但為抵禦不同類型 DDoS 攻擊手法，可再提高資源型耗盡偵測與阻擋機制，例如透過連線驗證或者是連線數管控等舒緩攻擊。在未來物聯網推波助瀾下，將有更多殭屍連網設備，可發動看似合法性的 DDoS 攻擊，在沒有特徵情況下，透過連線驗證與管控，並結合 GEO IP 資料庫進行封鎖都是未來防制選項必備條件。

本計畫將提供網路封包自動或手動特徵值阻擋應用層的資源耗盡攻擊，提供可支援連線數管控、連線驗證或依據國別 IP 資料庫，進行存取行為管制或區域性封鎖，來對抗大規模殭屍網路所引發的分散式阻斷服務攻擊(DDoS)。

5. HTTPS 網站內容瀏覽安全防護

全球超過一半的 web 流量改採用加密的 HTTPS 進行傳輸，意謂著對整個 web 進行加密傳輸已達到了一個里程碑時刻。駭客未來可能將攻擊躲藏在加密流量裡，藉此迴避偵測。為提升政府機關使用者上網安全，閘口設備必須提供可檢測 HTTPS 上網流量之設備，否則只能靠端點資安能量進行防護。

本計畫將佈建閘口 HTTPS Proxy 服務，各機關連線至 HTTPS 服務時，由該設備代理連線，並進行封包加解密檢測，用戶僅須信賴及安裝該設備憑證，即能受到保護，包括內容過濾掃毒、信譽黑名單阻擋，網站屬性分類、時間管理等防護。

6. DNS 快取伺服基礎建設安全防護

DNS 伺服器已躍升為主要遭受 DDoS 與其他攻擊類型的目標，「網域名稱系統」(DNS) 通訊協定在本質上便是容易遭受惡意探索的一個環節，單單在 2013 及 2014 年的 DNS 攻擊數目就增加了 200% 以上，全球中型與大型企業中就有 31% 的企業面臨至少一次 DDoS 攻擊，並有多家服務提供者與 DNS 主機服務提供者的 DNS 伺服器遭受 DDoS 攻擊而癱瘓。

本計畫提供多層級防護來對抗大規模殭屍網路所引發的分散式阻斷服務攻擊(DDoS)，對於 DNS 防護提供智能聰明的 DDoS 偵測技術、流量速率的限制，透過 DNS Firewall 針對已知的惡意網域提供一個彙整且即時資料更新的服務，阻擋企圖訪問存取這些惡意網域的惡意程式或使用者，並且取得已遭受感染裝置的情報，有效幫助管理者找出及修正單位裡潛藏的惡意程式攻擊來源。

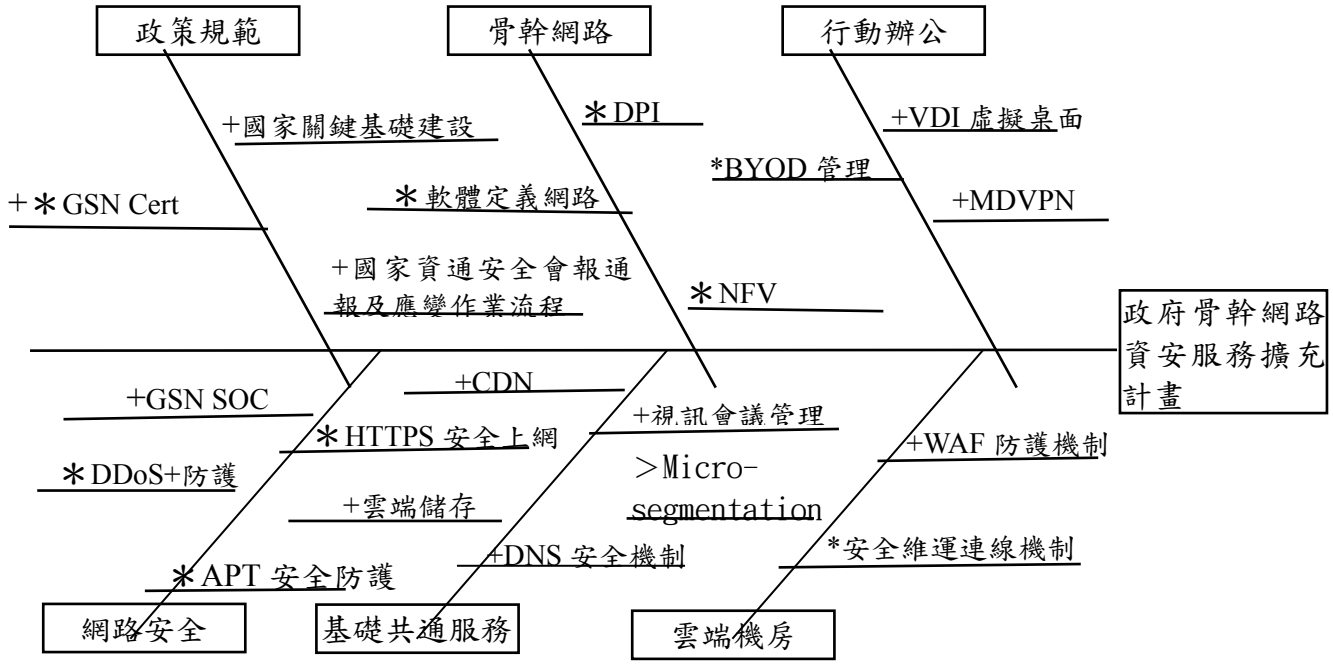
7. 廣域 DNS 快取伺服訊務負載平衡強化服務

本會已於 106 年度 6 月限制 GSN 內使用者僅能指向 GSN DNS，藉以強化 GSN 網路服務安全性，降低惡意及假冒網域造成機關傷害，因此 GSN DNS 系統可靠度及安全性將格外重要，本計畫將強化 GSN DNS 可用性及系統安全性，導入 SLB 及 Anycast 讓主機房及備援機房服務同時上線，若發生任何障礙可即時切換，達到服務可用率 100%的目標。

8. 行動化辦公安全性強化

隨著行動化裝置及網路逐漸普及，為推動政府行動化辦公服務，規劃建置虛擬化 SSL VPN 服務系統，依據導入機關需求自行調整內部安全政策，並統一開發雙因子認證機制，以強化服務安全性。

三、重要科技關聯圖例



(註) 科技成熟度之標註：

＋：我國已有之產品或技術

＊：我國正發展中之產品或技術

＞：我國尚未發展中產品或技術

產品或技術若與「智慧財產權」有關亦請加註說明

參、預期效益、主要績效指標(KPI)及目標值

一、預期效益：

(一) 建置骨幹級 DDoS 防護服務，確保政府機關遭受攻擊時能維持骨幹網路暢通，完善整體性縱深防禦機制，統計近年政府機關遭受 DDoS 攻擊次數超過 10 次計算，DDoS 防禦有效發揮其功效，如以地方縣(市)政府層級機關約 20 個估算，每年節省經費超過 1 億元(以機關自行建置 DDoS 防護系統費用約 500 萬估算，500 萬元*20)，如加計中央三、四級機關，節省費用更加可觀。

(二) 建置網頁應用防火牆(WAF)防護服務，提供 GSN 防護專區及行政院所屬委員會雲端資料中心網頁防火牆防護服務，除符合行政院資安政策要求 A、B 級機關須建置 WAF 機制，透過共同性防護，減少行政院所屬委員會雲端資料中心機關重複投資經費約 6,000 萬元（機關數 10 個計算，600 萬元*10）。

(三) 建置虛擬化 SSL VPN 服務系統及雙因子認證機制，強化服務安全性，各機關可依據不同需求自行調整內部安全政策，提供員工行動辦公室服務，透過安全連線機制，並通過安分驗證，可從遠端連線回機關內存取所需資源。

二、主要績效指標(KPI)：

計畫目標	績效指標	評估方式	衡量標準	107 年指標值
強化滲透攻擊防護及網頁過濾防護	提供網頁應用防火牆安全防護服務	數據統計	GSN DMZ 區用戶全數導入 WAF 防護	100%
		數據統計	辦理 1 場次網頁應用防火牆安全防護教育訓練	1 場次
提供骨幹端多層次網路防護	電路頻寬防護	數據統計	提供安全可靠的公務傳輸環境，完成行政院部會層級全數導入，避免機關遭受 DDoS 時其他機關連同遭受影響	100%
		數據統計	強化阻擋 DDoS 攻擊，提供連線管制功能系統可用率	99%
強化行動化辦公安全性	導入雙因子認證行動化辦公服務	數據統計	試辦 2 個部會導入雙因子認證行動化辦公服務	2 個部會
		數據統計	辦理 500 人次行動化辦公服務教育訓練	500 人次

三、目標值及評估方法：請說明本計畫 KPI 之目標值及評估方法。

上述三部分請填入分項目標與主要績效指標對照表。

目標	預算	預期成果效益	績效指標	評估方法	目標值訂定之依據
強化滲透攻擊防護及網頁過濾防護	3,500	提供GSN防護專區及行政院所屬委員會雲端資料中心網頁防火牆防護服務，除符合行政院資安政策要求A、B級機關須建置WAF機制，透過共同性防護，減少行政院所屬委員會雲端資料中心機關重複投資	提供網頁應用防火牆安全防護服務	數據統計	依據「國家關鍵基礎設施安全防護計畫指導綱要」，提供政府網際服務網骨幹網路之必要防護
提供骨幹端多層次網路防護	4,000	確保政府機關遭受攻擊時能維持骨幹網路暢通，完善整體性縱深防禦機制	電路頻寬防護	數據統計	依據「國家關鍵基礎設施安全防護計畫指導綱要」，提供政府網際服務網骨幹網路之必要防護
試辦行動化辦公服務	1,000	提供員工行動辦公室服務，透過安全連線機制，並通過安分驗證，可從遠端連線回機關內存取所需資源	導入雙因子認證行動化辦公服務	數據統計	試辦2個部會導入雙因子認證行動化辦公服務，並辦理500人次行動化辦公服務教育訓練

附件 3

前瞻基礎建設－數位建設

強化國家資安基礎建設之分項計畫

通傳會

106 年 7 月

壹、計畫緣起

一、政策依據

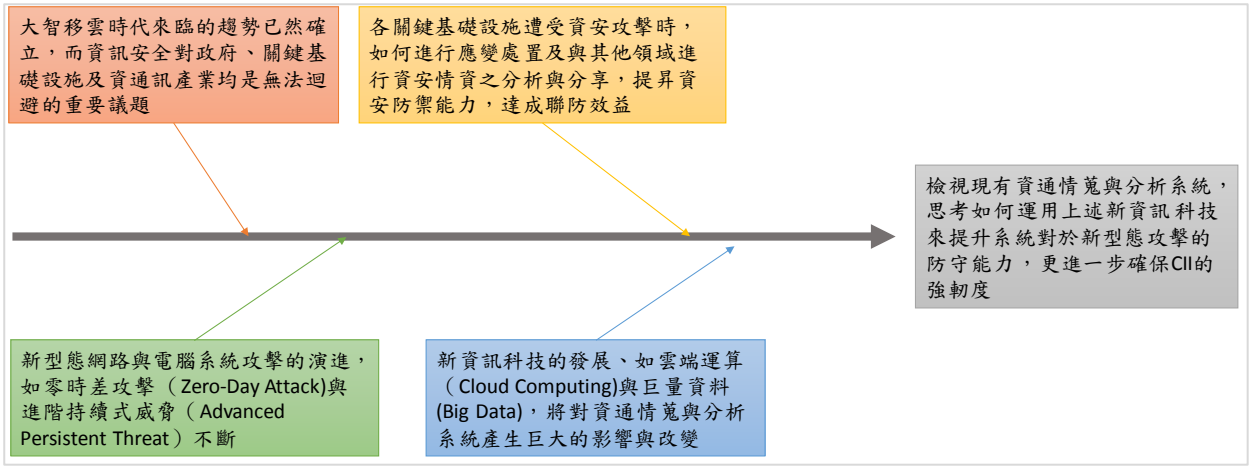
近年來，數位經濟帶動產業朝跨世代、跨境、跨領域、跨虛實等趨勢發展，促使全球產業格局翻轉。我國擁有厚實的工業基礎，面對數位經濟與物聯網(IOT)時代的來臨，建構完善的產業生態體系(ecosystem)，加速產業創新及優化產業結構，並充分利用我國既有優勢，進而掌握軟硬整合創新應用之契機，將是未來產業發展重點方向。

我國自 2002 年起推動國家資訊通信發展方案，至今逾 10 餘年，鑒於當前全球先進國家皆將數位經濟視為國家社會進步暨經濟轉型的主調，且政府目前推動產業創新及新南向政策，數位經濟為其重要驅動因素，「數位國家・創新經濟發展方案（2017-2025 年）」（簡稱 DIGI+），除延續之前國家資通訊發展方案，並在硬體與軟體建設並重原則下，透過建構有利數位創新之基礎環境，鞏固數位國家基磐配套措施，打造優質數位國家創新生態，以擴大我國數位經濟規模，達成發展平等活躍的網路社會，推進高值創新經濟並建構富裕數位國家之願景。

本計畫將配合《數位通訊傳播法》及《電信法》修正草案，建構通傳業者國家資通訊安全防護機制，強化數位匯流及資訊安全，培育跨域數位人才，提供民眾安全可信賴應用環境，為數位國家・創新經濟發展方案「數位創新基礎環境」工作主軸之一。並與與刻正規劃之第五期國家資通安全發展方案緊密銜接，規劃以「打造安全可信賴的數位經濟時代」為願景，並以「建置國家資安機制，提升自我防護能量」、「培育資安專業人才，推動資安產業發展」、及「建立資安防護團隊，保衛數位國家安全」為目標，透過「完備資安基礎環境」、「建構國家資安聯防體系」、「推升資安產業自主能量」、「孕育優質資安菁英人才」4 項策略，推動執行各項工作。

二、擬解決問題之釐清

大智移雲（大數據、智能化、移動網際網路和雲端運算）時代來臨，根據美國「戰略暨國際政策研究中心(Center for Strategic and International Studies, CSIS)」於 2010 年委託資安公司 Mcafee 之調查報告(In the Crossfire - Critical Infrastructure in the Age of Cyber War)指出，全世界各關鍵基礎設施多曾遭受各式威脅與攻擊。2010 年起，伊朗核設施工業控制(Supervisory Control and Data Acquisition, SCADA)系統遭惡意不法組織以 Stuxnet 病毒攻擊，感染約三萬台以上電腦，導致伊朗納坦茲核設施的五分之一離心機被迫關閉，重創伊朗核子計畫。2011 年 Stuxnet 之變種病毒 Duqu 蠕蟲出現，此惡意程式專門用於蒐集工業控制系統製造商之情資與擷取鍵盤敲擊在內之數位情報，以便未來對工業控制系統所控管之關鍵基礎設施發動攻擊。未來各國在關鍵資訊基礎建設所面臨的，將是更趨複雜且難以獨自處理的複合式威脅。



圖表 1　目前遭遇的問題

三、環境需求分析

關鍵基礎建設(Critical Infrastructure, CI)，泛指一個國家為了維持民生、經濟與政府等相關運作而提供之基本設施與服務，包括實體以及以資訊電子為基礎之系統，為重要社會基礎功能所需之基礎建設。關鍵資訊基礎建設(Critical Information Infrastructure, CII)保護不僅僅是領域內各機構的協同保護，亦牽涉到跨領域的協同合作。落實資安防護最重要的基本功夫，就是必須要能夠了解臺灣整體面臨的資安威脅現況，並能針對不同領域所遭受到威脅進行分析與分享。本計畫內容為強化通傳領域關鍵資訊基礎設施安全狀態掌握，包括 SOC、ISAC 及 CERT 等平臺擴建或建置，協助通傳業者關鍵資訊基礎建設建立集中式資安問題監控、情資分享與緊急應變，將有助於提升國家整體資安防護能力。

四、計畫定位

為落實「資安即國安」的政策方針，本會與國家安全會議資通安全辦公室及行政院資通安全處共同為政府資安鐵三角，推動我國資通安全工作，其中關鍵基礎設施安全和帶動臺灣資安產業發展為施政重點。本會除規劃建置資通安全防護中心，透過電視牆，即時掌握通傳業者 CI 資安現況外，更透過本計畫推動關鍵基礎設施資安防護，發展防護基本政策與防護基準，建立 CII 關鍵基礎設施領域之資安訊息分析分享中心(ISAC)、資安通報應處平臺(CERT)及資通安全中心(SOC)，預期將可提升 CI 及 CII 通傳業者對於資安事件預警、監控、應變和處理能力等，落實通訊傳播事業關鍵資訊基礎設施的資安防護，擴大國家資安聯防的機制，確保臺灣的資安防護能力，達成資安鐵三角之效益。

貳、計畫目標

一、目標說明

因應每天數以萬計的資安事件及系統紀錄等需要被處理或管理，國內通傳事業(包含電信業者、ISP 業者、有線電視業者…等)為了保護重要資源，均已建立各種資安防護系統來抵禦外部攻擊，常見設施包含有：防火牆、防毒軟體、虛擬私人網路(VPN)、安全掃描以及入侵偵測系統(IPS)、入侵防禦系統(IDS)，網路應

用程式防火牆(WAF)等，已廣泛運用在資安環境上。

本分項計畫預計整合資安技術與相關軟硬體建置，建立並維運通傳資通安全中心(SOC)維運管理平臺，彙集多元資安情資來源，制定通傳事業資安事件應變處理機制(CERT)，提供資安事件分析、資安趨勢、資安關聯之情資分享(ISAC)，提升整體通傳事業資通安全水準，降低資安事件衍生之風險，保障國內資通安全與人民權益。

二、執行策略及方法

資安事件監控與通報平臺運作：藉由誘捕系統佈建及同時針對誘捕能量之提升，增加佈點主機 IASP 家數，以及未來擴大規模，提升資安事件分析、強化資安弱點管理與資安事件追蹤與通報，以達到通傳事業資通安全能量之提升。

垃圾郵件防制監控與通報平臺運作：於通傳事業垃圾郵件之處置，除了藉由成立通傳資通安全中心及垃圾郵件處理中心外，為強化垃圾郵件之管理，並能針對惡意郵件處置與分析，於佈點主機上增設 SPAM 誘捕技術，以 Container 為核心之配置架構、可規模化倉儲與分析平臺，以因應快速複製及未來擴大建置之需求，以提升通傳事業垃圾郵件管理之效率。

資安情資分析分享完整機制之建立：藉由 C-ISAC 平臺之建立，並與 N-ISAC、其他領域 IASC、國內外情資來源之資訊蒐集，即時獲得資安情資，並就通訊傳播相關之資安議題，透過邀請合作單位（例如：中科院、資策會、大專院校學術單位、資安社群組織）針對情資進行進一步研析，並據此獲得行動方案，透過協調國內通傳事業單位進行改善，以即時強化通訊傳播資通安全防禦能力。

本計畫分項目標及細部計畫名稱如下，執行策略說明如後：

表格 1　分項工作說明

分項目標	細部計畫名稱
建置 CIIP 新一代資通安全中心(C-SOC)	擴增通傳事業佈點主機及垃圾郵件之誘捕系統(5＋7 家) 完成新一代資通安全中心(C-SOC)資料備份及異地備援機制 完成新一代資通安全中心(C-SOC)系統效能監控平臺
建置 CIIP 新一代通報應處平臺(C-CERT)	完成通傳事業 CIIP 新一代資安訊息通報應處平臺(C-CERT)
建置 CIIP 新一代資安訊息分析分享中心(C-ISAC)	完成新一代資安訊息分析分享中心(C-ISAC) 完成新一代資通安全宣導網站

分項工作說明

建置 CIIP 新一代資通安全中心(C-SOC)

本計畫將完成通傳資通安全中心(以下簡稱 C-SOC)相關能量之建立，包含管理制度之導入，備援備份系統之建置，以及通傳資通安全中心 C-SOC 自身系統運作情形監控之設置，相關工作事項說明如下：

擴增通傳事業佈點主機及垃圾郵件之誘捕系統(5＋7 家)

本會 106 年已先建置 C-SOC 前期功能驗證，及五家 IASP 業者佈點主機經由技服中心產生資安告警事件之接收驗證，本計畫規劃於 107 年，除於原有 5 家佈點主機外（中華電信、遠傳速博、亞太電信、台灣固網、台灣碩網），增設網際網路服務（IASP）10 萬戶以上用戶之 IASP 業者 7 家，以及擴增其誘捕能力，同時佈點主機蒐集之誘捕資訊，採直接方式接入 C-SOC，分別完成資安事件、垃圾郵件佈點主機所收集之威脅日誌，C-SOC 系統配合其功能之擴充，將由 C-SOC 接收威脅日誌取得後透過一線監控及二線分析能量，完成佈點主機誘捕作業與威脅資訊之分析與彙集。

完成新一代資通安全中心(C-SOC)資料備份及異地備援機制

為提升通傳資通安全中心**(C-SOC)**整體系統運作可靠度，以及系統服務之可用性與災難復原能力，本計畫規劃於 107 年度擴大業務執行範圍，強化既有環境之復原能力及建置異地備援環境。

為能有效管理及備份資料並在災難發生時迅速復原運作環境，以穩定的方式完成每日繁複的備份工作。本項工作將建置單一介面備份管理系統，統一控管所有實體主機及虛擬環境主機重要資料備份管理機制，依據不同需求將資料存放於磁帶、磁碟或者異地儲存空間。一體化及自動化的備份管理機制有助於資通安全中心降低繁複資料備份工作，並可於災難發生時迅速找到對的資料，快速恢復系統運作。

為能符合 107 年相關平臺建置之需求，資通安全中心基礎設備、環境、架構亦需配合進行系統擴充規劃，於備援備份規劃考量亦須將整體擴充需求一併考量，以滿足平臺擴增所需之容量與效能。

完成新一代資通安全中心(C-SOC)系統效能監控平臺

通傳資通安全中心之日常營運作業中，除了針對資安事件與垃圾郵件進行事件監控與分析外，資通安全中心運作服務本身亦需要透過監控各系統的運作狀態以利維持正常運作狀態之掌握，透過系統監控平臺之建立，於系統運作發生異常時，能夠第一時間即時掌握與處置，降低異常之衝擊，同時亦能事前異常的發現以及事先問題處理，減少系統失能之風險，若系統不慎發生障礙，也能即時通知相關人員處理，即時監控各系統健康狀態及系統資源使用情況。

效能監控需包含：環境、網路節點、作業系統、資料庫系統、應用程式等，以下就各層面效能監控摘要說明之，107 年將依其重要性決定導入的優先順序，並分年分階段完成之。

環境：建置數位監視系統，以監視及錄影機櫃內實際運作情形。

網路節點：監控系統各網路節點健康狀態及網路頻寬使用率，使用者人數增加時，網路流量也會隨著增加，其流量若大於網路線的頻寬，系統效能將降低，造成有

些訊息可能會延遲傳送。

作業系統：建立各種資源(CPU、RAM、Network、Storage 等)的使用趨勢，進而適當調整資源之使用或進行擴充。

應用程式：監控關鍵資訊系統的反應時間(Response Time)，當使用者人數增加後，在網路頻寬足夠的情況下，系統的反應時間若超過可接受的範圍，則必須提前做出改善作為。

資料庫系統：各資料庫系統本身已具備相關的效能監控機制，實務上往往存在多種資料庫系統，其中有套裝軟體綁定的資料庫系統，也有自行規劃建置的，若單靠個別資料庫系統本身所提供之工具可能較不方便，因此擬建置異質資料庫管理工具以簡化管理。

建置 CIIP 新一代通報應處平臺(C-CERT)

為協助提供網際網路之通傳事業於面臨所管理之網路環境下遭受到惡意攻擊之情事，可透過通傳資通安全中心所建置之通報應處平臺進行緊急通報，並藉由標準交換格式進行相關資訊交換，經由 C-SOC 進行緊急事件分析，當事件攻擊來源於國內時，主動通知該網路服務之管理業者進行緊急處置，並進行後續的追蹤與回報，當事件攻擊來源發生於國外時，藉由 N-CERT 向合作國或對等 CERT 機構進行反映。

完成通傳事業 CIIP 新一代資安訊息通報應處平臺(C-CERT)

本計畫規劃於 107 年完成新一代資安訊息通報應處平臺**(C-CERT)**，將採用 106 年所制定之新一代訊息交換格式（STIX）並因應通傳事業所需之訊息交換需求完成建立訊息交換介面與系統平臺。新一代資安訊息通報應處平臺同時包含並滿足

兩大元件所需之功能：
能符合適用於通傳事業之資安監控系統進行資訊界接所需，包含通報、追蹤及應處回覆。

需與資通安全中心 C-SOC 事件監控分析進行整合，包含實體系統之整合及運作流程管控，並透過 C-SOC 事件單開立與追蹤管理，完成通報應處程序。

建置 CIIP 新一代資安訊息分析分享中心(C-ISAC)

本項工作於 107 年將透過佈點主機誘捕系統之佈建、完成資安資訊分享與分析系統之規劃與建置、以及民眾舉報平臺之建立，透過與 N-ISAC 會員情資交換，完成通傳事業之資安聯防機制之建立，相關工作事項說明如下：

完成新一代資安訊息分析分享中心(C-ISAC)

本項目將配合技服中心所制訂之規格完成 TAXII 系統建置，並與技服中心所建置之新一代資安訊息分析分享平台（N-ISAC），以新一代資料交換技術及規格（STIX、TAXII、CybOX）完成五種情報交換測試，五種情報種類包含有：資安訊息情報（ANA）、網頁攻擊情報（DEF）、入侵攻擊情報（INT）、資安預警情報（EWA）、資安回饋情報（FBI），同時依據該規格為基礎完成與五家 IASP 業者交換格式差異性規劃、C-ISAC 完整情資交換架構與平臺規劃。

針對 C-ISAC 完整平臺系統、IASP 業者端情資交換介面之建置，107 年度將將優先與既有 5 家 IASP 業者（中華電信、遠傳速博、亞太電信、台灣固網、台灣碩網）完成資安情資分享系統介接，並擴增網際網路服務（IASP）十萬用戶以上業者 7 家，共計 12 家完成資安情資分享運作機制，及事件通報與處置回報自動化作業。

完成新一代資通安全宣導網站

建立新一代通訊傳播資通安全宣導網站，同時藉由整合資通安全中心各角色（C-SOC、C-CERT、C-ISAC）所蒐集或取得各式資安情報資料，透過行動方案之建立，將資安事件與垃圾郵件防治手段分享，透過資安事件與垃圾郵件宣導，提升民眾資安相關意識，藉此強化通傳事業整體資安防護意識，及積極預防事件擴大。

關鍵因素分析

茲針對本計畫 SWOT 分析方法分析本規劃內部之優勢(Strengths)、劣勢(Weaknesses)、外部之機會(Opportunities)和威脅(Threats)，進而擬定因應之發展策略，以掌握內在優勢，克服內在弱勢，利用外部機會並避開外部威脅，SWOT 分析如下表所示。

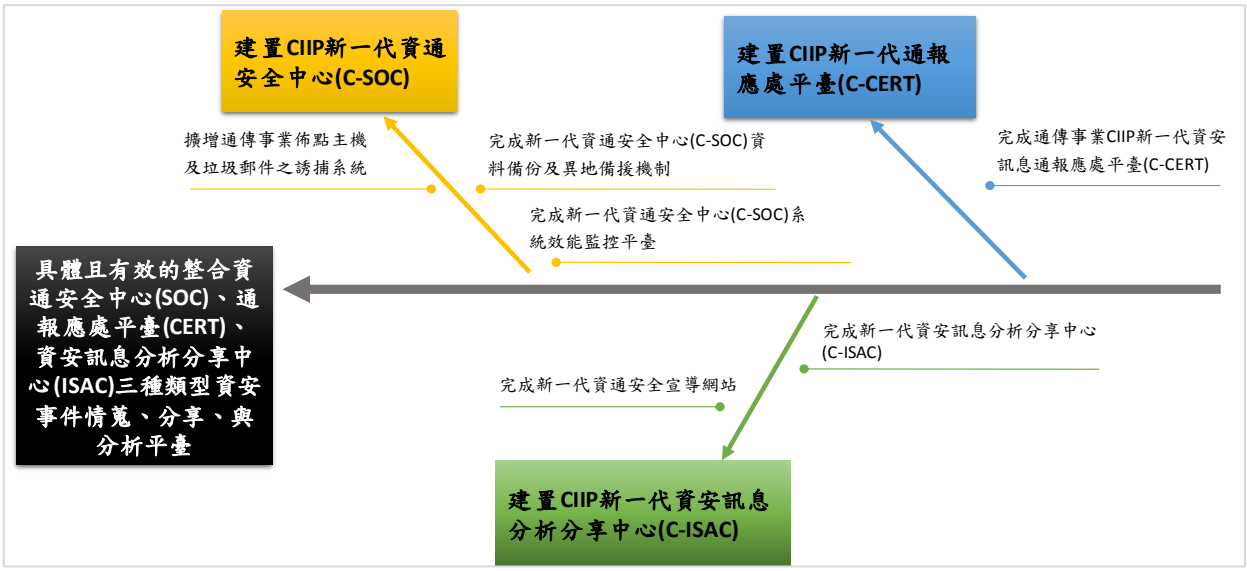
表格 2　SWOT 分析(B001)

SWOT 分析	
優勢(Strength)	劣勢(Weakness)
通傳事業網路資安威脅逐漸受業者及消費大眾重視，有助於本計畫執行 通傳會長期研究電信網路資安及系統效能，具備相關能力，可有效整合通傳業者共同參與計畫，達成設定目標 本計畫與刻正規劃之第五期國家資通安全發展方案緊密銜接，屬前瞻基礎建設之一環	通傳事業網路資安事件多樣化且隨時有新型態攻擊出現，相關安全防護準則須具備時效性 通傳事業網路 24 小時進行運作，安全防護能力不易驗證 通傳事業之資安事件發生後，才進行通報，通傳會係被動知悉，未能即時掌握第一時間之資安狀態
機會(Opportunity)	威脅(Threat)

提升全體通傳事業關鍵基礎設施資安防護能力，降低資安事件損失 培養通傳事業關鍵基礎設施資通安全防護，協助相關資安產業發展	監控通傳事業關鍵基礎設施運作、通報或進行應變處置時若涉及商業機密及損失時，其中權衡(Trade-off)不易決定 通傳事業關鍵基礎設施資通安全防護能力與投入經費資源有絕對關係，業者配合程度為執行成敗關鍵因素之一

目標實現時間規劃

本計畫為一年期之計畫，計畫目標說明如下：

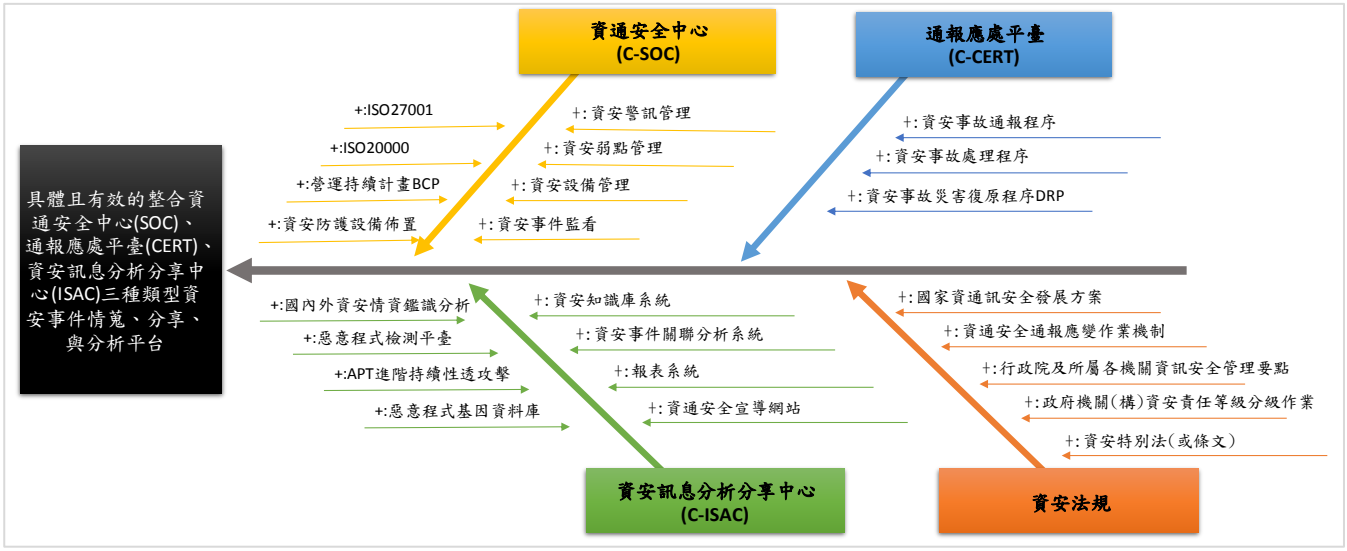


圖表 2　計畫目標圖

表格 3　分項目標說明

分項目標	第一年目標	期末目標	長期目標
建置 CIIP 新一代資通安全中心 (C-SOC)	擴增通傳事業佈點主機及垃圾郵件之誘捕系統(5＋7 家) 完成新一代資通安全中心(C-SOC)資料備份及異地備援機制 完成新一代資通安全中心(C-SOC)系統效能監控平臺	藉由 C-SOC 資安事件之蒐集及 N-ISAC 成員之技術分享，完成建置資安事件知識庫，以建立大數據分析能量 優化資安事件與垃圾郵件誘捕系統誘捕能量	以「建置國家資安機制，提升自我防護能量」、「培育資安專業人才，推動資安產業發展」、及「建立資安防護團隊，保衛數位國家安全」為目標，並透過「完備資安基礎環境」、「建構國家資安聯防體系」、「推升資安產業自主能量」、「孕育優質資安菁英人才」4 項策略，推動執行各項工作。
建置 CIIP 新一代通報應處平臺 (C-CERT)	完成通傳事業 CIIP 新一代資安訊息通報應處平臺(C-CERT)	定期查核電信事業防護基準落實情形 舉辦資安攻防演練，確認通傳業者通報應處之應變能量	
建置 CIIP 新一代資安訊息分析分享中心 (C-ISAC)	完成新一代資安訊息分析分享中心(C-ISAC) 完成新一代資通安全宣導網站	完成資安事件知識庫及數位鑑識平臺 參與資安技術交流並持續推動培訓資通安全資安事件分析與資安鑑識人才，並取得資安事件分析與鑑識相關證照資格	

重要科技關聯圖例



圖表 3　重要科技關聯圖

(註) 科技成熟度之標註：

＋：我國已有之產品或技術

＊：我國正發展中之產品或技術

＞：我國尚未發展中產品或技術

產品或技術若與「智慧財產權」有關亦請加註說明

參、預期效益、主要績效指標(KPI)及目標值

一、預期效益：

本項計畫藉由研析先進國家通傳事業於資安監控與通報機制、垃圾郵件防制作法，同時分析我國實務執行面之差異，同時與通傳事業業者溝通及邀請加入通傳資通安全中心及情資分享計畫，完成建立通傳資通安全中心及資安訊息分析交換平臺，對於特殊事件資安威脅、情資分析，及建立垃圾郵件分析中心及監控平臺，以提升通傳事業整體垃圾郵件之防制，及資安威脅情報綜整能協助通傳事業及早因應防範資安事件擴大。

二、主要績效指標(KPI)：

請以表列方式說明本計畫之績效指標並將其與計畫目標相對應。

三、目標值及評估方法：

請說明本計畫 KPI 之目標值及評估方法。

表格 4　主要績效指標及評估方法說明

目標	預算	預期成果效益	績效指標	評估方法	目標依據
建置 CIIP 新一代資通安全中心 (C-SOC)	60,000 仟元	擴增通傳事業佈點主機及垃圾郵件之誘捕系統(5＋7家) 完成新一代資通安全中心(C-SOC)資料備份及異地備援機制 完成新一代資通安全中心(C-SOC)系統效能監控平臺	H.技術報告及檢驗方法：建置數位匯流資通安全分析管理平臺技術報告 S2.科研設施建置及服務：資通安全中心(C-SOC)完成 12 家 ISP 佈點主機整合納入	依建置完成之實體平臺及通傳業者介接數進行評估	依前瞻基礎建設 - 數位建設 4.1.4 強化國家資安基礎建設計畫執行本計畫
建置 CIIP 新一代通報應處平臺 (C-CERT)		完成通傳事業 CIIP 新一代資安訊息通報應處平臺(C-CERT)			
建置 CIIP 新一代資安訊息分析分享中心 (C-ISAC)		完成新一代資安訊息分析分享中心(C-ISAC) 完成新一代資通安全宣導網站	AB.科技知識普及：建置新一代資安事件與垃圾郵件宣導網站及情資分享平臺		

表格 5　主要績效指標表(KPI)(B003)

屬性	績效指標	初級產出量化值	預期效益說明
學術成就（科）	A.論文		

屬性	績效指標		初級產出量化值	預期效益說明
	B.合作團隊(計畫)養成		培養資通安全分析團隊 1 組	進行數位匯流資通安全分析管理平臺自主營運
	C.培育及延攬人才			
	D1.研究報告			
	D2.臨床試驗			
	E.辦理學術活動			
	F.課程/教材/手冊/軟體			
	其他			
技術創新(科技技術創新)	G.智慧財產			
	H.技術報告及檢驗方法			
	I1.辦理技術活動		辦理通傳事業 ISAC、CERT 採用新一代情資交換技術（STIX、TAXII）說明會 3 場次	
	I2.參與技術活動		專家會議 6 場次 參與國際 Anti SPAM 技術研討活動	邀請產官學及專家學者就通傳事業資通安全當前面臨之關鍵基礎設施資安議題發表意見
	J1.技轉與智財授權			
	J2.技術輸入			
	S.技術服務(含委託案及工業服務)			
	S2.科研設施建置及服務		完成 12 家 ISP 佈點主機整合納入	
	其他			
經濟效益（經濟產業促進）	L.促成投資			
	M.創新產業或模式建立			
	N.協助提升我國產業全球地位			
	O.共通/檢測技術服務及輔導			
	P.創業育成			
	T.促成與學界或產業團體合作研究			
	U.促成智財權資金融通			
	AC.減少災害損失			
	其他			
社會影響	社會福祉提升	科普知識推廣與宣導(次數、觸達人數)、新聞稿刊登篇數、媒體宣傳數量	建置新一代資安事件與垃圾郵件宣導網站(Ⅳ) 建置惡意程式基因資料庫及情資分享平臺(Ⅳ)	
		設立網站數、提供客服件數、知識或資訊擴散(觸達)人次、開放資料(Open Data)項數與筆數、提供共用服務或應用服務項目數、線上申辦服務數	建置新一代資安事件與垃圾郵件舉報網站(Ⅳ) 建置通傳事業資安事件與垃圾郵件通報應處系統(Ⅳ)	
		廠商增聘人數		
		旅行時間節省(換算為貨幣價值)		

屬性	績效指標		初級產出量化值	預期效益說明
		受益人數、增加收入(金額)		
		人權、弱勢族群或性別平等促進活動場次、參與人數		
	環境安全永續	技術或產品之能源效率提升百分比；技術/產品達成綠色設計件數；提升新能源及再生能源產出量		
		包含國土、環境、健康等各式調查之調查點筆數、圖幅數、面積、影像資料筆數、物種數等		
其他效益（科技政策管理及其他）	K.規範/標準或政策/法規草案制訂		制訂通傳事業 CII 情資交換標準	
	Y.資訊平台與資料庫		建置惡意程式基因資料庫及情資分享平臺 建置新一代惡意程式檢測平臺完成自動化檢測機制	
	AA.決策依據		通傳事業 CII 資通安全防護之執行審視，俾供通傳會決策參考	
	其他			