

114 年度區域網路中心年終成果基礎資料彙整表

高屏澎 區域網路中心

(負責學校：國立中山大學)

114 年 11 月 20 日

目錄

壹、基礎維運資料.....	2
貳、網路管理.....	7
參、資安服務.....	19
肆、特色服務.....	23
伍、前(113)年度執行成效評量改進意見項目成效精進情形	34
附表 1：區網網路架構圖	36
附表 2：連線資訊詳細表	37

壹、基礎維運資料

一、本部補助經費與人力

區域網路 中心經費 使用(114 年度)	1.教育部核定計畫金額：新臺幣 <u>4,710,000</u> 元 2.教育部補助計畫金額：新臺幣 <u>4,710,000</u> 元 3.區域網路中心自籌額：新臺幣 <u>0</u> 元，補助比率 <u>100</u> %。 4.實際累計執行數(1月至10月)：新臺幣 <u>3,344,951</u> 元，執行率 <u>71</u> %。
區域網路 中心人力 運作	專任： <u>5</u> 人，兼任： <u>0</u> 人。 其中包含教育部補助： 1.網路管理人員： <u>3</u> 人，證照數： <u>1</u> 張。 2.資安管理人員： <u>2</u> 人，證照數： <u>2</u> 張。 3.雲端管理人員： <u>0</u> 人，證照數： <u>0</u> 張。(無者免填)

二、本部補助經費使用情形與績效檢討。

說明：

1.請填寫本(114)年度(截至10月)經費預計達成率。

2.檢討前3年度(111-113)達成率。(如有經費繳回，請簡述原因)。

年度	達成率	繳回金額	說明
114	71%		
113	77%	375,000	專任助理離職人力替補空窗期結餘款
112	100%	0	依計畫編列內容完整報支
111	100%	0	依計畫編列內容完整報支

1.本(114)年度預計達成率為100%。

2.113年度本計畫專任助理離職，因人力替補空窗期，繳回結餘款375,000元。

三、本部補助貴區網中心之網管、資安及雲端人力等服務績效。

說明：

1.請填寫前3年度(111-113)及本年度(114)人事經費運作(人員配置及異動)情形。

2.檢討歷年度人事經費運作(人員異動因素；另如人事經費有繳回，請述明原因)。

年度	專任人力	兼任人力	網管人員
114	10人	0人	3人
113	8人	1人	1人
112	9人	3人	1人
111	9人	3人	1人

1.教育部補助網管人員，主要負責項目如下：

- 區網IPv6服務建置及推動

- 區網設備維護如 Cisco 核心路由器、DNS 服務伺服器及 VoIP
- 區網設備及網管系統每日監控、維護、穩定度測試及參數修正：包含簡訊管理系統、Cacti、PRTG 網管系統維護，連線異常處理。
- Log 訊息管理系統
- 辦理連線單位頻寬升速事宜
- 區網相關會議及研討會工作辦理、協助、發文等作業
- 區網 VM 服務系統維護
- 網路流量分流設備維護及管理
- 舉辦區網中心管理會議及技術分享會議
- 黑名單系統開發及分享
- Google Cache Service (GGC)服務新主機上線，後續管理及維護。

2.教育部補助資安人員，主要負責項目如下：

- 辦理網站弱點掃描服務改版作業
- 資安及個資稽核認證導入及維護證書有效性(ISO 27001認證)
- 資安及個資相關政策維運及各項表單維護修改
- 辦理區域網路中心暨縣(市)教育網路中心業務持續運作(Business Continuity Plan)演練計畫
- DNS版本升級及資安健檢服務執行
- 協助連線單位處理資安事件，包含攻擊手法分析及資安鑑識等
- 辦理資安通報審核處理
- 網頁偵測置換規則系統建置
- DDOS協助清洗
- C2惡意流量系統規劃及建置

3.檢討歷年度人事經費運作(人員異動因素，如人事經費有繳回，請述明原因)。

無。

四、預估 115 年度經費與人力營運規劃。

說明：如各項人力超過 2 位以上，請說明分工、原因及必要性。

區域網路中心 經費(115 年度)	1.預計申請教育部補助經費：新臺幣 <u>4,710,000</u> 元。 2.預計區域網路中心自籌額：新臺幣 <u>0</u> 元。
區域網路中心 人力運作	專任：共 <u>5</u> 人，兼任：共 <u>0</u> 人。 其中包含教育部補助： 1.基礎維運(網管)人員： <u>1</u> 人，證照數： <u>1</u> 張。 2.基礎維運(資安)人員： <u>2</u> 人，證照數： <u>1</u> 張。 3.教育雲管理人員： <u>0</u> 人，證照數： <u>0</u> 張。 4.雲端(CDN)管理人員： <u>2</u> 人，證照數： <u>0</u> 張。

五、其它基礎資料(網路管理及資安管理)

請依下列項目提供本(114)年度報告資料

(一)區域網路中心連線資訊彙整表

	項目		縣(市)教育網中心	大專校院	高中職校	國中小學	非學校之連線單位 (不含 ISP)	總計
(1)下游連線學校或連線單位數統計	連線學校(單位)數		3	26	2	0	1	連線單位總數：
	連線單位比例		7.5%	85%	5%	0%	2.5%	註：單位數 / 總數
(2)連線頻寬與電路數統計	專線(非光纖)		0	0	0	0	0	
	光纖	10M(不含)以下	0	0	0	0	0	
		10M(含)以上 100M(不含)以下	0	0	0	0	0	
		100M(含)以上 500M(不含)以下	0	2	1	0	0	
		500M(含)以上 1G(不含)以下	0	4	0	0	0	
		1G(含)以上 10G(不含)以下	0	19	1	0	1	
		10G(含)以上	14	1	0	0	0	
	其他(如 ADSL 等)		0	0	0	0	0	
	連線電路小計		14	26	2	0	1	
	連線頻寬合計 (電路實際租用頻寬加總)		140G	32.5G	1.3G	0	1G	連線頻寬總計：
								174.8G
	連線頻寬比率		80%	18%	1%	0%	1%	請加總電路實際租用頻寬/總計頻寬

	項目		縣(市)教育網中心	大專校院	高中職校	國中小學	非學校之連線單位 (不含 ISP)	總計	
(3)連線縣(市)教育網路中心	縣(市)教育網路中心			連線頻寬				合計	
	1.	高雄市教育局網路中心		連線頻寬(遠傳)			40G	90G	
				連線頻寬(中華)			50G		
	2.	屏東縣教育網路中心		連線頻寬(遠傳)			20G		
				連線頻寬(中華)			20G		
	3.	澎湖縣教育網路中心		連線頻寬(遠傳)			0G		
連線頻寬(中華)				5G					
(4)非學校之連線單位(不含 ISP)	連線單位名稱			連線頻寬				備註	
	1.	高雄榮民總醫院		1G					
	2.								
	3.								
	4.								
	5.								
	6.								
	7.								
	8.								
	9.								
	10.								
(5)連線 TANet		主節點名稱		連線頻寬				備註	
	1.	_____ 台南 _____ 主節點		100G					
	2.	_____ 台中 _____ 主節點		100G					
(6)其他線路	ISP 名稱(AS)			連線電路數		連線頻寬(合計)		備註	
	1.	中華電信 Hinet(AS3456)		1		10G			
	2.	新世紀資通 Seednet(AS4780)		1		500M			
	3.	新世紀資通 NCIC(AS9919)		1		1G			
	4.	台灣固網 TFN(AS9964)		1		1G			
	5.	遠傳電信 APG(AS17709)		1		100M			
	6.	GGC server		2		20G			
	7.								
	8.								
(7)補充說明									
(8)連線資訊	請依附表「學校/單位連線資訊詳細表」格式填附								

(二)區域網路中心資訊安全環境整備表

(1)區域網路中心及連線學校資安事件緊急通報處理之效率及通報率。 (請向教育部資科司資安科窗口取得數據)	資安責任等級： <u>B</u> (核定日期：)。 1、2 級資安事件處理： (1)通報平均時數： <u>0.13</u> 小時。 (2)應變處理平均時數： <u>0.07</u> 小時。 (3)事件處理平均時數： <u>1</u> 小時。 (4)通報完成率： <u>100</u> 。 (5)事件完成率： <u>100</u> 。 3、4 級資安事件通報： (1)通報平均時數： <u>無</u> 小時。 (2)應變處理平均時數： <u>無</u> 小時。 (3)事件處理平均時數： <u>無</u> 小時。 (4)通報完成率： <u>無</u> 。 (5)事件完成率： <u>無</u> 。 資安事件通報審核平均時數： <u>6.03</u> 小時。
(2)區域網路中心配合本部資安政策。 (請向教育部資科司資安科窗口取得數據)	1.資通安全通報應變平台之所屬學校及單位的聯絡相關資訊完整度： <u>100</u> %。 2.區網網路中心依資通安全應執行事項： (1)是否符合防護縱深要求? ☒是 ☐否 (2)是否符合稽核要求? ☒是 ☐否 (3)符合資安專業證照人數： <u>2</u> 員 (4)維護之主要網站進行安全弱點檢測比率： <u>100</u> %。

(三)區域網路中心維運事項辦理情形及目標

(相關補充或詳細說明可於報告時陳述)

項目	本(114)年度辦理情形	明年目標
(1)召開區管理會之辦理情形及成果 (含連線單位出席率、會議召開次數)。	召開次數： <u>2</u> 次 出席率： <u>70</u> %	召開次數： <u>2</u> 次 預期出席率： <u>75</u> %
(2)骨幹基礎環境之妥善率。	<u>100</u> %	<u>100</u> %
(3)連線學校之網路妥善率。	<u>100</u> %	<u>100</u> %

(4)辦理相關人員之專業技術推廣訓練。	場次：共 <u>4</u> 場 人次：共 <u>100</u> 人次	預計場次：共 <u>4</u> 場 預計人次：共 <u>100</u> 人次
(5)連線學校之 IPv4/IPv6 推動完成率。	<u>94</u> %	<u>97</u> %
協助連線學校之網管及資安工作:		
● 建立區網路維運管理機制。	主要管理機制為何(請簡述)：建立網路監控機制供下轄學校觀看，並建立斷線通知監控、與下轄學校建立 LINE 群組，有任何問題可來電或於群組上詢問。	未來管理機制(維持或新增)(請簡述)：更新並建立新的網路監控軟體，以及維持與下轄學校的良好互動。
● 協助連線學校網路的維運或障礙排除(含諮詢)。	<u>156</u> 次	<u>140</u> 次
● 建立資安防護或弱掃服務 (含諮詢)(達成率百分比)。	<u>100</u> % (共 <u>32</u> 所，完成 <u>32</u> 所)	<u>100</u> % (共 <u>32</u> 所，預計完成 <u>32</u> 所)
● 建立連線學校相關人員聯繫管道及聯絡名冊。	共 <u>32</u> 所，達成幾所： <u>32</u>	共 <u>32</u> 所，達成幾所： <u>32</u>
(6)服務滿意度(百分比)。	<u>100</u> %	<u>100</u> %
(7)其他。		

貳、網路管理

請詳述貴中心之網路連線、網管策略及具體辦理事項

說明：

1.114 年度網路管理維運具體辦理事項。

2.115 年度網路管理營運方針。

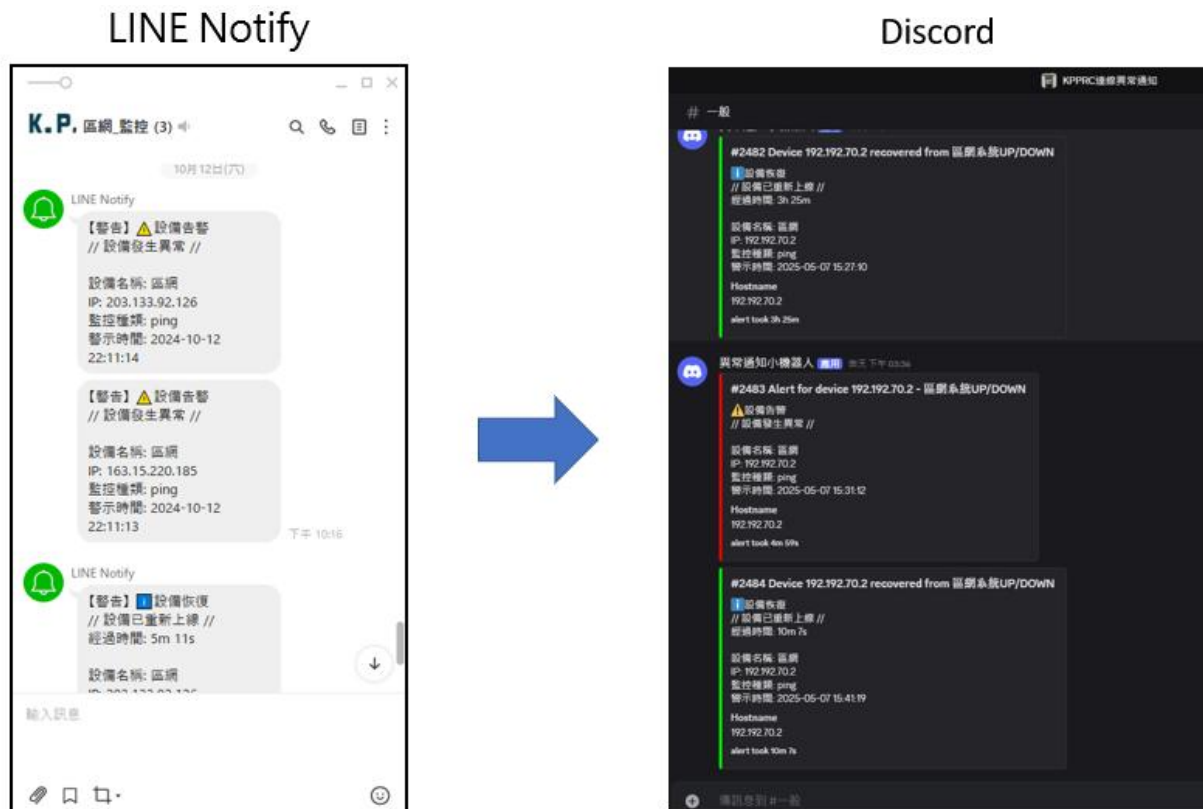
一、114 年度網路管理維運具體辦理事項

(一)協助下轄骨幹頻寬更新

- 1.協助美和科技大學線路改接：於 1 月 13 日協助美和科技大學將原中華電信 200M 線路調整為台灣大哥大 1G 連線，提升網路頻寬與穩定度。
- 2.中斷和春科技大學 TANet 服務：與和春科技大學確認後，於 4 月 11 日正式停止 TANet 連線服務，並將相關 IP 資源歸還教育部。
- 3.中華電信卡版升級：於 9 月 25 日完成高屏澎區網中心中華電信機房之卡版升級作業，確保設備運作穩定並提升系統效能。
- 4.針對所屬連線單位進行 IP、介面及頻寬資料之盤點與更新作業，並透過電話確認相關資訊。

(二)Discord 區網監控

1. 因應 LINE Notify 終止服務，改用 Discord 監控網路有無斷線，以便斷線後立即處理。



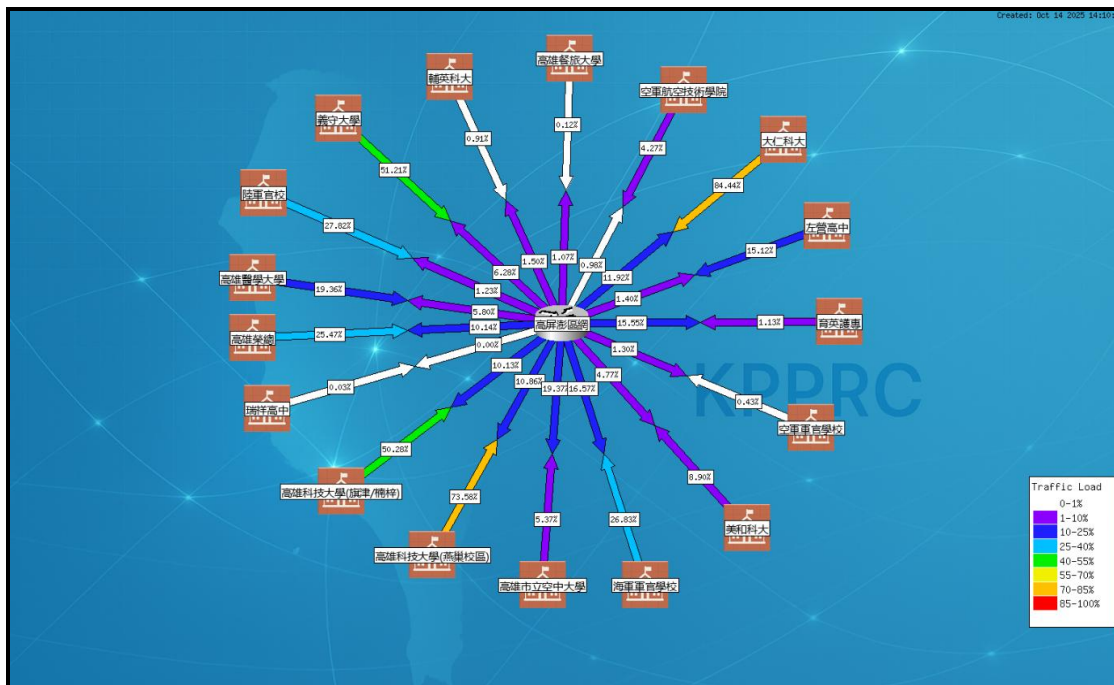
(三)網路流量監控設備建置及更新

1. Cacti重新建置：舊實體主機的Cacti監控軟體停機，改為虛擬主機並建置新的Cacti監控軟體。

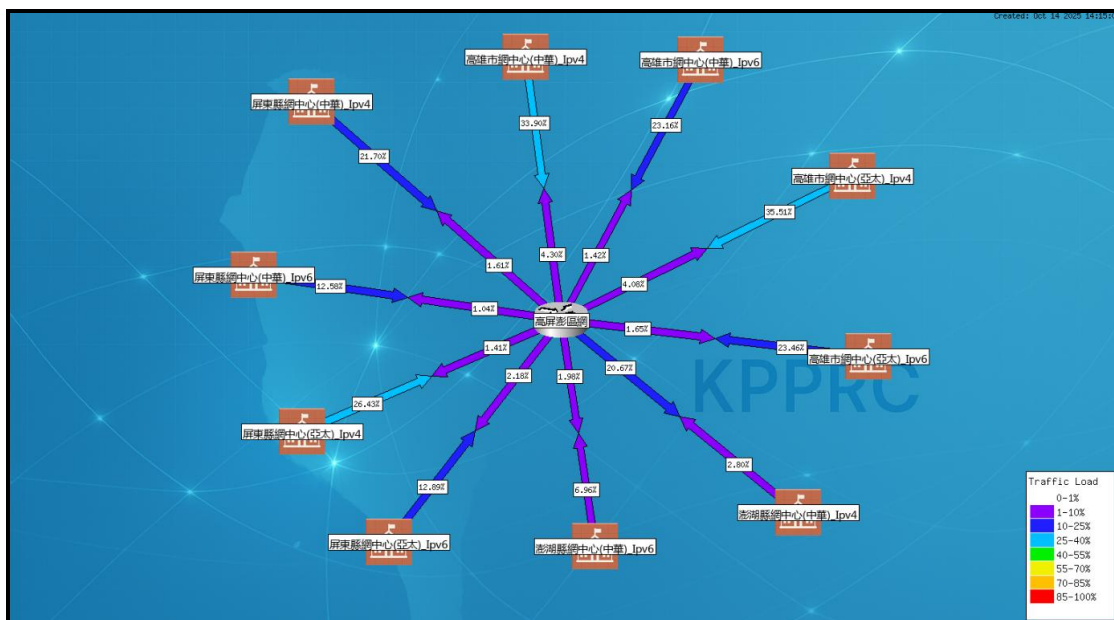


2. 建置Weather Map：建置新的Weather MAP

(1) 下轄連線單位

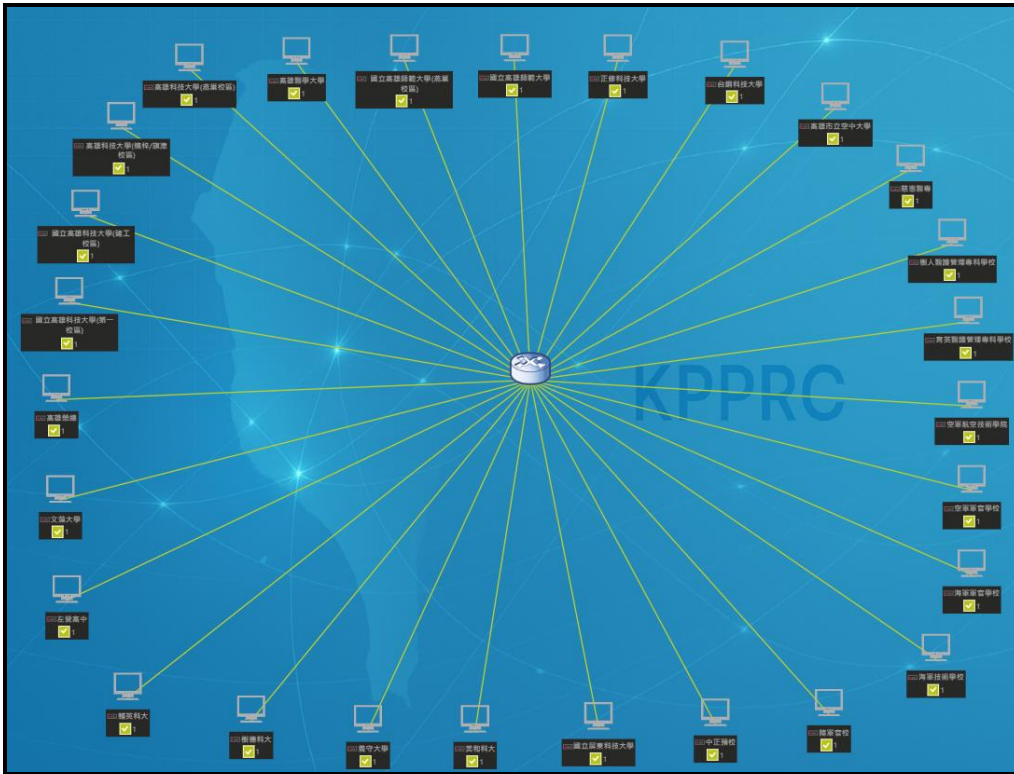


(2) 縣網連線單位

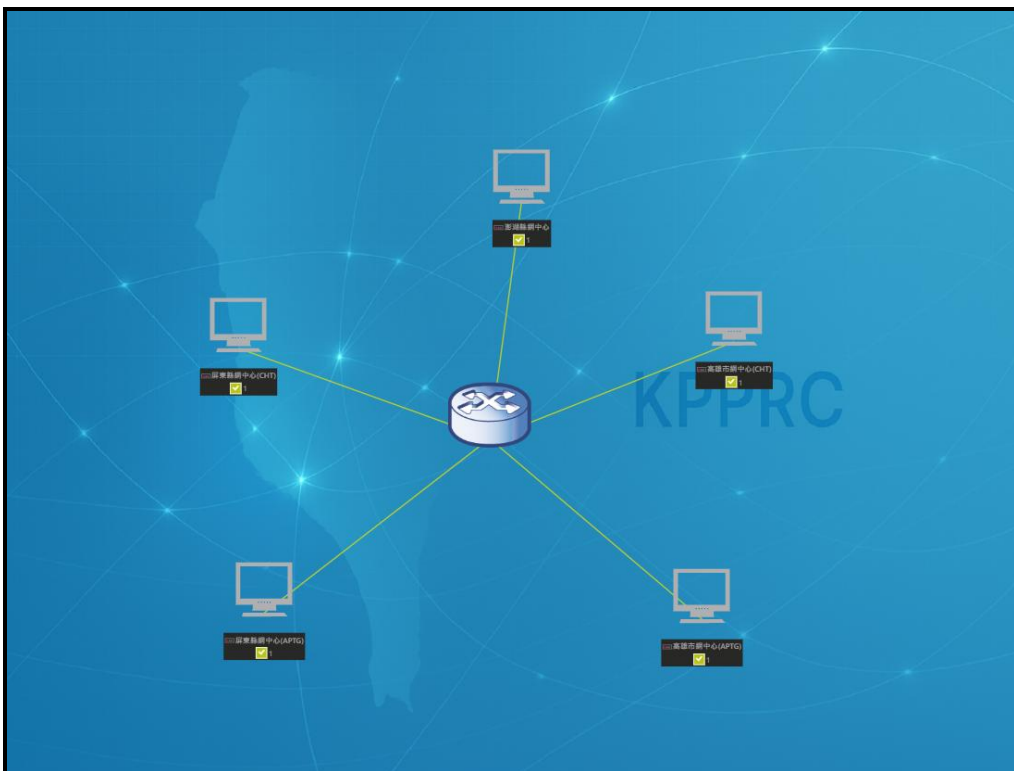


3. PRTG網路監控建置：建置新的PRTG網路以即時監控斷線與延遲。

(3) 下轄連線單位



(4) 縣網連線單位

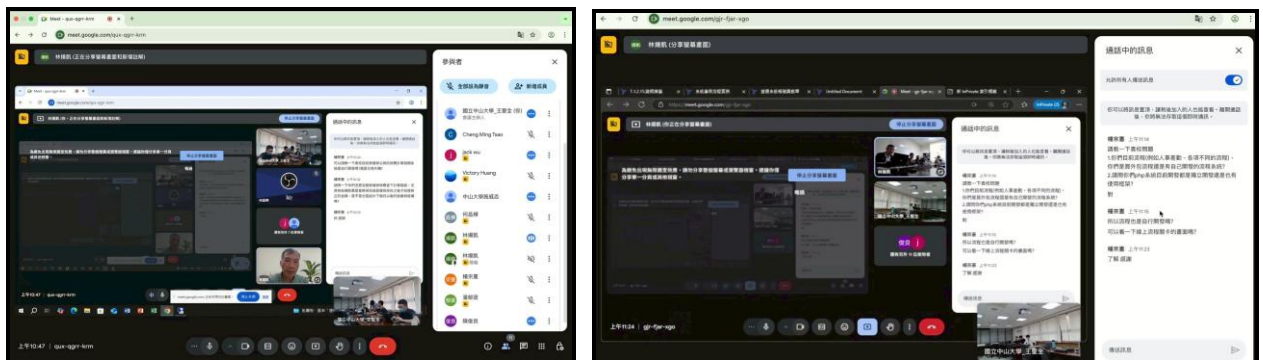


(5)網路延遲及斷線通知提醒

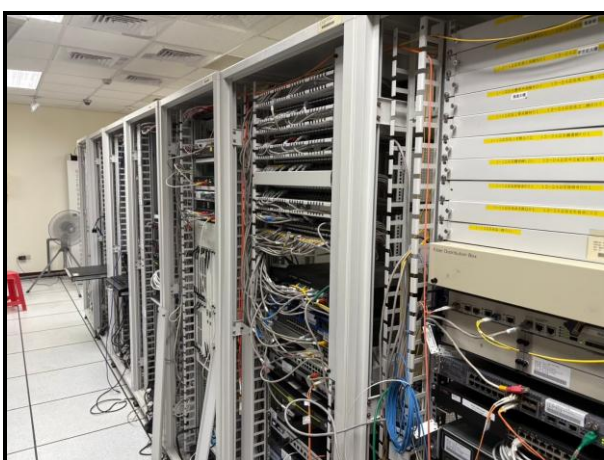
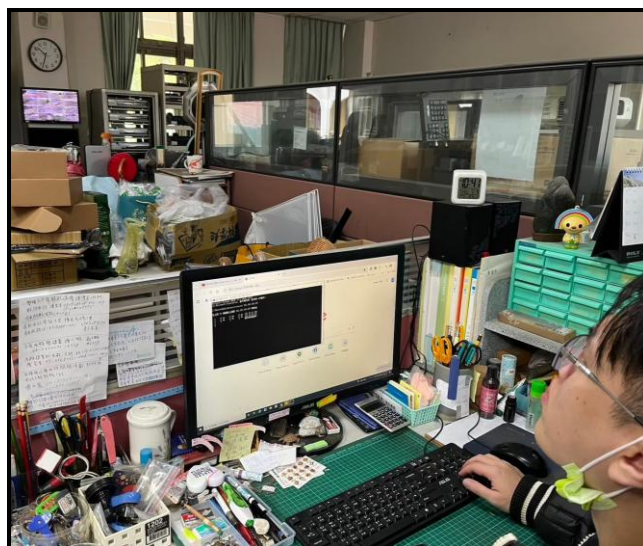
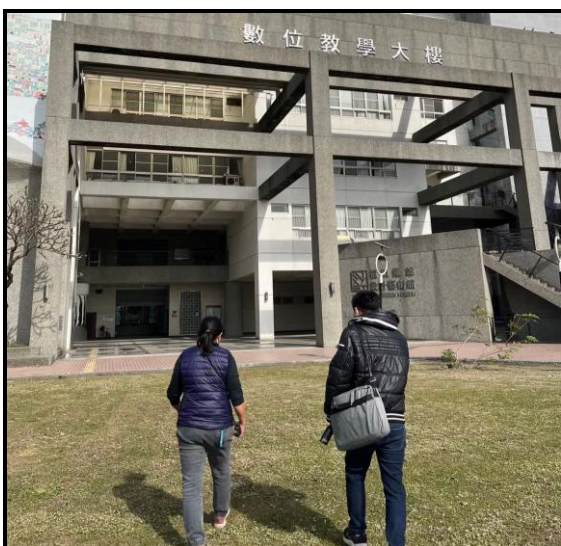


(四)與下轄連線單位交流與服務

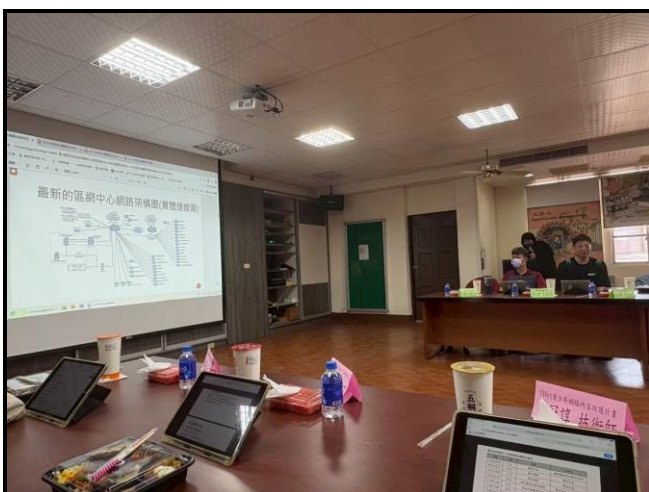
- 1.與高雄醫學大學開線上技術交流會議：4、5月與高雄醫學大學網路組、系統組開線上會議，彼此交流技術與問題，一起討論提升能力。

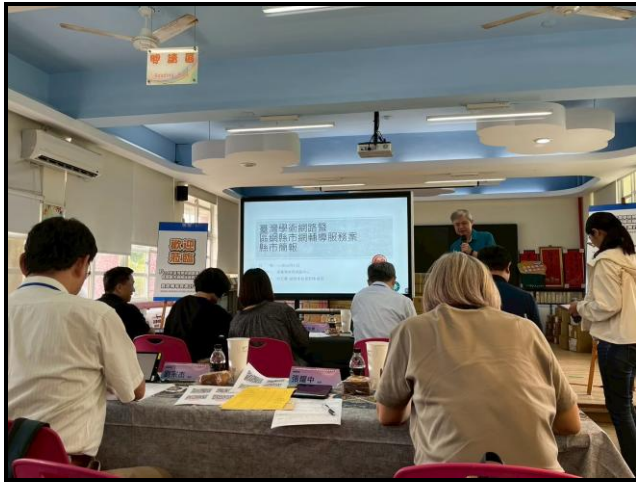


- 2.關閉東方設計學院網路設備：協助東方設計學院盤點並關閉不必要之網路設備，以降低資安風險並維持網路有效運作。由於該校目前已無專責網管人員，本中心持續提供相關技術協助與諮詢服務。



3. 高雄市網、屏東縣網訪視：協同教育部進行高雄市網、屏東縣網訪視工作，加強雙方交流與合作，並深化彼此對網路運作及管理現況之了解。



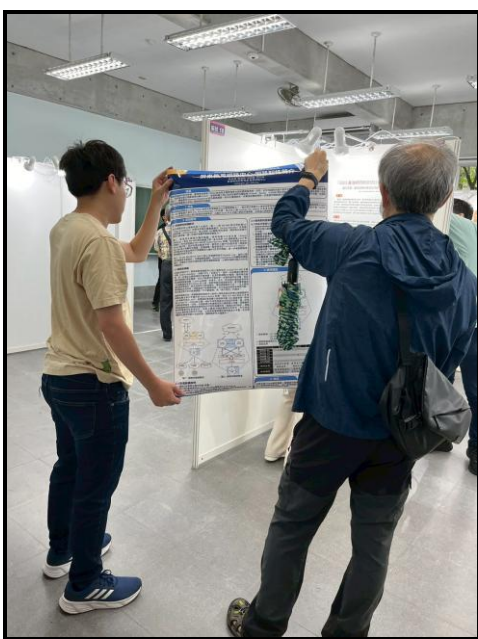


4. 協助屏東縣網中心解決網路流量異常問題：與屏東縣網路中心組長及網管人員共同討論，並透過 Log 資料進行分析，發現一台未使用的設備產生異常高流量。經協調後移除該設備，成功排除流量異常問題。





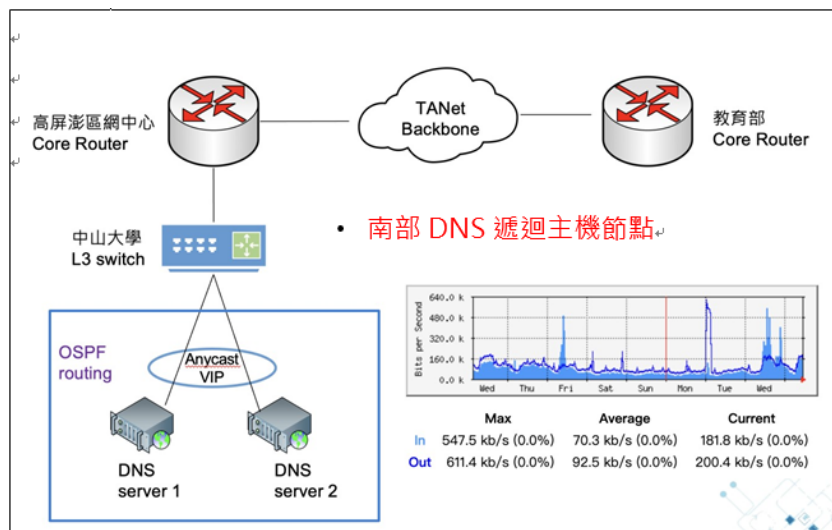
5. 參與 TANet 2025 研討會活動：與屏東縣網路中心共同參加 TANet 2025 研討會活動，並合作投稿一篇海報論文，分享網路韌性，促進技術交流。





(五)續維運教育部 DNS 主機

1. 台中以南學術網路將以中山遞迴主機為主進行查詢，降低北部負載，提升學術網路效率。
2. 本中心為求服務穩定，另建置HA架構SWITCH，力求能穩定提供服務。
3. DNS遞迴主機查詢服務，同時提供HA服務；當北部據點無法查詢時，本中心據點可做為備援服務。
4. 建置架構如下：



(六)連線單位異常反應處理

1.114 年 2 月高雄大學 DNS 受 DDOS 攻擊：

- 原因：2月5日17點11分學校DNS受到DDOS攻擊，經過流量清洗有緩解。
- 處理結果：後續回報學校並持續觀察流量，2月5日17點45分確認流量恢復正常。

2.114 年 5 月澎湖縣網中心反映斷線：

- 原因：5月17日12點30分澎湖縣網中心反映斷線，經查詢路由器以及與中華電信確認，判斷為中

華電信陸纜故障。

- 處理結果：通知中華電信人員並於高屏澎區網中心網站公告，確認於5月17日15點50分修復完畢。

3.114 年 7 月左營高中反映網路延遲：

- 原因：7月14日15點10分左營高中老師反映網路延遲，與左營高中老師討論，可能為左營端的中華電信設備故障。
- 處理結果：協調中華電信人員去左營高中更換數據機，經再次網路交叉測試確認，7月14日17點00分確認恢復連線。

4.114 年 9 月高雄科技大學 IoT 對外暴露：

- 原因：因不少IoT暴露在外，去電詢問狀況與原因，得知掃描IoT困難。
- 處理結果：提供我方IoT掃描技術文件，供連線單位參考。

5.114 年 10 月高雄餐旅大學不定時斷線及網路不穩：

- 原因：10月8日上午11點18分來訊息通知近日常有高延遲及斷線等問題，經判斷為路由器設備上GBIC問題，訂好於11月15日12點10分更換設備。
- 處理結果：更換路由器上GBIC設備後持續觀察，11月15日12點17分確認恢復網路穩定度。

6.114 年 10 月育英醫專不定時斷線及網路不穩：

- 原因：10月15日上午9點00分詢問育英醫專，因以前提過偶爾會斷線及網路不穩，是否要更換GBIC看看，後訂於10月20日下午5點更換。
- 處理結果：更換路由器上GBIC設備後持續觀察，10月20日下午5點13分確認恢復網路穩定度。

(七)教育訓練辦理

時間	主題
05 月 23 日	舊瓶裝新酒：持續演變的 DNS 服務與資安議題探討
07 月 21 日	零信任(Zero Trust)與數據(data)安全
09 月 18 日	資安與你我的距離，外部攻擊行為的識別與防護
11 月 10 日	物聯網裝置安全初探

(八)管審會議與教育訓練調整

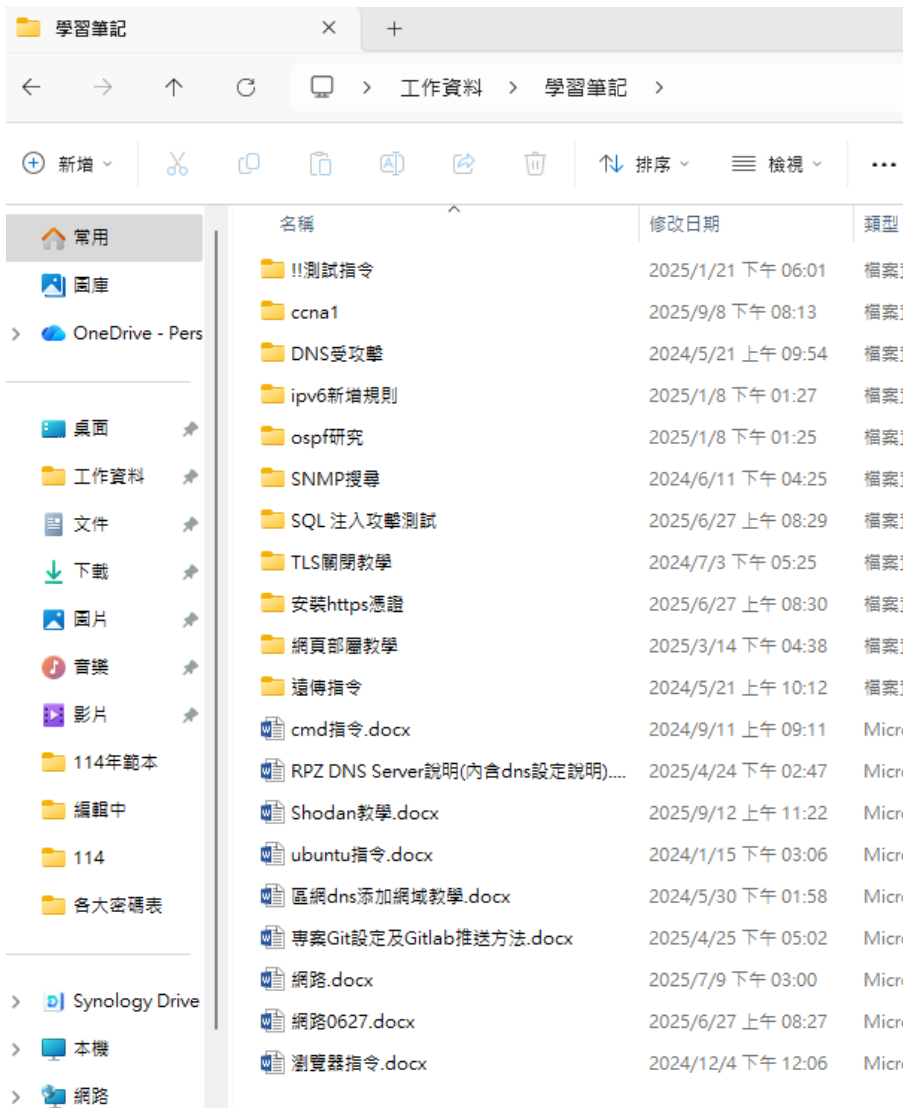
- 1.調整演講議程時間：經回饋上午通常較繁忙，故調整為下午辦理。
- 2.調整管審會議參與方式：期中管審會議參與人數不如預期，打電話關心每位未參與人員，發現原因為人力資源過少，無法空出一整天出席參與；因此期末調整方式也提供線上會議連結，讓沒辦法全程出席的人可以線上參與。
- 3.調整管審會議報告內容：新增技術與工具分享，分享好用的工具及自己撰寫的腳本，或是技術教學文件，供連線單位學習與參考。

(九)人員專業能力提升：加強人員專業能力提升服務專業度

- 1.建立下轄學校異常連線紀錄表：詳細記錄問題發生時間、處理方式與完成時間，作為後續故障排除與經驗回饋之依據，提升未來類似事件的處理效率與應變速度。

桌面 > 工作資料 > 區網 > 異常連線處理紀錄 > 114 >				
搜尋				
工具(T)				
名稱	修改日期	類型	大小	
1140411和春技術學院正式退場	2025/10/14 下午 03:28	檔案資料夾		
1140509阿帕契資安漏洞	2025/10/15 下午 05:31	檔案資料夾		
1140108資安單預期16小時.docx	2025/1/8 下午 02:24	Microsoft Word ...	92 KB	
1140113美和線路由中華電信改為台灣大哥大.docx	2025/10/14 下午 01:38	Microsoft Word ...	52 KB	
1140122收到三信家商情資.docx	2025/8/1 上午 10:41	Microsoft Word ...	1,445 KB	
1140205高雄大學dns受ddos攻擊.docx	2025/10/15 下午 05:19	Microsoft Word ...	437 KB	
1140304教育部遠傳roteing受cldap放大攻擊.docx	2025/3/4 下午 03:39	Microsoft Word ...	76 KB	
1140414資安單逾時.docx	2025/4/14 上午 11:14	Microsoft Word ...	230 KB	
1140415 資安單逾時.docx	2025/4/15 上午 09:13	Microsoft Word ...	185 KB	
1140427資安單(半夜)遲時.docx	2025/4/28 上午 09:30	Microsoft Word ...	296 KB	
1140507澎湖斷線.docx	2025/5/14 上午 10:23	Microsoft Word ...	138 KB	
1140710屏東技術支援(中瀝屍病毒).docx	2025/7/15 上午 10:48	Microsoft Word ...	1,295 KB	
1140714左營高中網路延遲.docx	2025/7/15 上午 10:36	Microsoft Word ...	14 KB	
1140909資安單存查.docx	2025/9/10 下午 02:08	Microsoft Word ...	957 KB	
1140912高科大一校區iot掃描問題.docx	2025/10/14 上午 11:24	Microsoft Word ...	63 KB	
1141013高雄客運大學網路都會陸陸續續斷線或不穩....	2025/10/14 上午 11:29	Microsoft Word ...	128 KB	

2.建立教學文件檔：如IoT掃描、FTP匿名掃描、Gigamon使用、ASR9010常用指令、常用網路指令、DNS建置及修改教學等。



3.參加課程考取專業證照：CCNA1、CEH。

CCNA1



CEH

Test History	
Certified Ethical Hacker	
Candidate Name	ZUHN SHE
Test Name	Certified Ethical Hacker
Test Taken Date	31 October, 2025
Gained Score	124
Final Result	Passed

二、115 年度網路管理營運方針

- (一)透過到點服務加強與下轄學校的連結，安排專人前往現場提供技術支援與協助，並主動詢問學校的意見與需求，增進資安管理的即時性與互動性。
- (二)部分連線單位因預算有限，其監控設備因長期經費問題無法有效獲得維護，仰賴自建服務，本中心將持續精進，各項監測服務系統如NETBOX、N-Reporter sflow，提供給需要的連線單位使用，以使連線單位在有限經費預算下，也能夠同時擁有良好的網路監測與異常管理能力。
- (三)未來將加強與下轄學校的資訊互通性，詳細記錄連線異常原因、狀態及處理結果，並於之後的管審會中進行分享，讓大家更關注近期頻繁發生的異常狀況。

- (四)於管審會分享更多自己遇到的狀況及教學文件、技術工具提供，加深與連線單位互動性與技術提升。
- (五)加強人員培訓，提升專業能力，如考取CCNA證照，使其更熟練且快速地處理問題，並提供更全面及更多的服務。

參、資安服務

請詳述貴中心之資安服務、資安政策及具體辦理事項

說明：

- 1.114 年度資安服務維運具體辦理事項。
- 2.115 年度資安服務目標(實施措施)。

一、114 年度資安服務維運具體辦理事項

(一)協助資安通報平台問題協助與反映

1. 資安事件單一小時內完成執行困難：

- 原因：下轄學校反映，資安事件單通報時間時常為非上班時間，又有一小時內需通報完成問題，在執行上有難度。
- 處理：已與Tacert協調，可以調整知悉時間，計算時間方式為知悉時間至通報時間，並告知下轄學校。

2. 詢問資安事件處理方式：

- 原因：針對資安事件處理，諮詢適當的解決方法。
- 處理：提供其他學校或本校的相關做法作為參考。

(二)ANA 事件單通知信轉發與諮詢

1. 將ANA事件單通知信共282封轉發給各下轄資安人員，如有問題提供協助與諮詢。

(三)SOC 中心 IoT 暴露名單轉發與諮詢

1. 將每月IoT暴露事件單通知信轉發給各下轄資安人員，如有問題提供協助與諮詢。
2. 提供掃描IoT技術文件供下轄連線單位參考。

(四)協助 DDOS 流量清洗

1. 協助DDOS流量清洗申請：

事件類型統計		轄下單位密碼更動情況		DDOS清洗系統		演練事件單		轄下單位資安長表	
清洗IP*									
DNS IP									
單位名稱*	高屏區域網路中心								
通訊協定*	TCP								
服務說明*	例如:WEB FTP								
通訊埠*	例如:80								
申請理由									
送出 (本系統僅適用於TANET部份地區)									

OID查詢							
威脅名單	事件事件列表	EWA列表	事件類型統計	輕下單位電腦更新情況	DDOS清洗系統	黑名單管理	黑名單事件
新進申請單							
編號	申請時間	清洗IP	通訊協定	通訊埠	狀態	檢視	
136	2020-10-05 11:46:24		TCP/UDP	53		檢視	
137	2020-10-06 14:17:55		tcp	53		檢視	
138	2020-10-06 16:09:50		udp	udp, random port		檢視	
139	2020-10-07 10:13:54		udp	80		檢視	
140	2020-10-07 13:55:53		tcp	80		檢視	
146	2021-02-23 11:55:54		tcp	80		檢視	
147	2021-02-24 13:41:55		tcp	80		檢視	
148	2021-02-24 23:13:00		tcp	80		檢視	
149	2021-02-25 11:07:49		tcp	80		檢視	
150	2021-02-25 14:00:54		tcp	80		檢視	
151	2021-02-25 14:13:42		tcp	80		檢視	
152	2021-03-02 13:35:09		udp	random port		檢視	
153	2021-03-02 13:51:36		tcp	80		檢視	
163	2021-10-03 16:23:19	194.1	tcp	80		檢視	
166	2022-03-16 17:00:42		tcp	80		檢視	
178	2022-08-16 17:21:56		tcp	80 443		檢視	
186	2022-09-12 08:56:14		tcp	80	處理完成	檢視	
246	2024-05-14 20:24:35		udp	80	處理完成	檢視	
247	2024-05-17 15:55:14		TCP/UDP	53	處理完成	檢視	
248	2024-05-18 09:24:52		tcp	53	處理完成	檢視	
249	2024-05-18 13:55:08		TCP/UDP	53	處理完成	檢視	
257	2024-06-19 15:20:09		TCP/UDP	all	處理完成	檢視	
263	2025-02-05 17:17:08		TCP/UDP	53	處理完成	檢視	
264	2025-02-05 17:17:36		TCP/UDP	53	處理完成	檢視	
267	2025-03-28 09:56:11	210	tcp	53		檢視	
268	2025-03-28 09:56:55		TCP/UDP	53		檢視	
269	2025-03-28 09:58:01		udp	53		檢視	

(五)黑名單共享系統

1. 建立黑名單共享系統：匯集下轄學校提報的惡意網域及IP，透過人工審核集結成清冊，再供下轄學校使用。

我的上傳檔案

我的黑名單

黑名單下載

上傳檔案管理

黑名單管理

上傳網域黑名單

使用者管理

管理者

黑名單系統

新增上傳教育部網域黑名單功能

網域名稱黑名單 (TXT 檔)

選擇檔案

未選擇任何檔案

送出

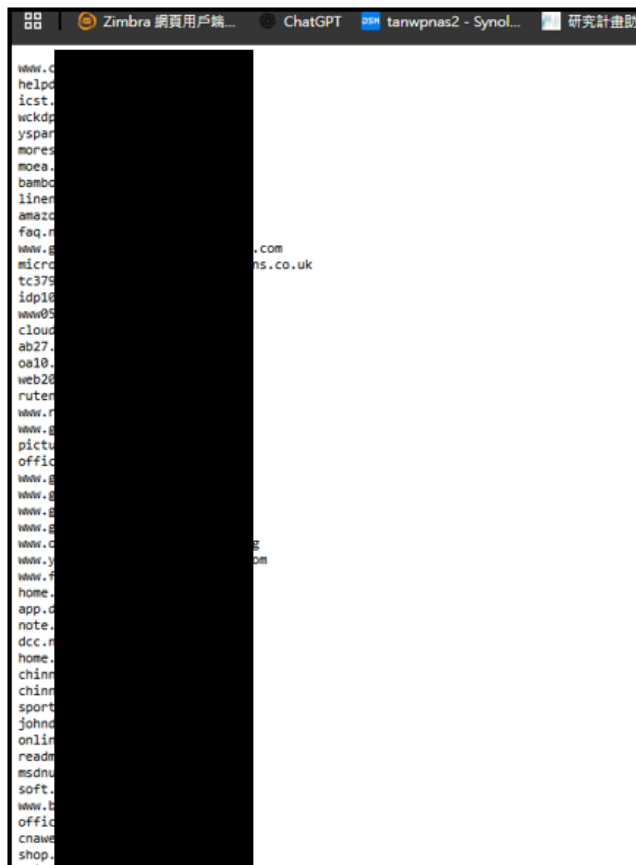
網域名稱黑名單 TXT 文字檔網址

<https://blacklis>

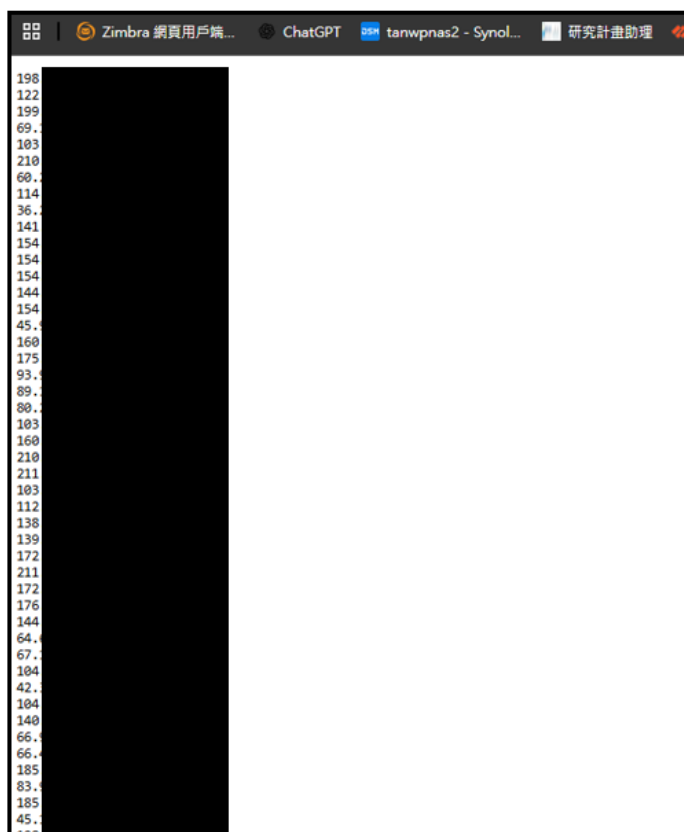
📄 下載 Excel 檔 📄 下載 CSV 檔 📄 下載 ODS 檔 🌐 網域黑名單 最後更新時間： 2025-10-15 14:58:08	
黑名單 IP ↑↓	被列入黑名單的原因 ↑↓
154.23.221.136	Botnet
199.204.99.106	Back.Orifice.Traffic
45.192.208.126	Botnet
202.79.175.117	Botnet
192.253.229.124	Botnet
176.65.149.231	Mirai.Botnet Multiple.Routers.GPON.formLogin.Remote.Command.Injection Realtek.SDK.UDPServer.Command.Execution Remote.CMD.Shell SSH.Connection
118.86.231.105	Zyxel.Firmware.error.message.Command.Injection
195.3.223.82	Netcore.Netis.Devices.Hardcoded.Password.Security.Bypass
93.203.238.208	Zyxel.Firmware.error.message.Command.Injection
	APISIX.Admin.API.default.token.Remote.Code.Execution APSystems.ECU-R.timezone.Command.Injection ASUS.GT-AC2900.asus_token.Authentication.Bypass 45195.Remote.Code.Execution Apache.OFBiz.Endpoints.Incorrect.Authorization.Code.Execution Apache.OFBiz.getJSONuiLabel.SSRF Apache.Options.bleed 8442.Information.Disclosure Aviatrix.Controller.File.Upload.Path.Traversal Aviatrix.Controller.cloud_type.Command.Injection Avtech.Devices.HTTP.Request.Flood 1653.Information.Disclosure Cisco.Smart.Licensing.Utility.Static.Credential.Security.Bypass Citrix.Application.Delivery.Controller.VPNs.Path.Traversal Citrix.Application.Delivery.Controller.VPNs.Path.Traversal

2.提供惡意網域引用網站，供下轄學校引用至防火牆或下載，有設排程自動更新教育部惡意網域黑名單及IP。

(1)教育部惡意網域黑名單



(2) 教育部惡意IP黑名單



二、115 年度資安服務目標(實施措施)

(一)提供資安問題協助與技術交流

- 加強與下轄學校之資安技術交流與支援，彙整並提供 IoT 弱掃、FTP 匿名檢測、SQLi 與 XSS 等教學與操作文件，並提供弱點掃描工具安裝與使用示例、檢測結果判讀與優先修補建議；同時於管審會議提供技術分享，並提供個別諮詢與必要之到點支援，協助現場修補與強化設定，提升資安防護能力。

(二)黑名單共享系統

- 完善黑名單共享系統，調查下轄學校的使用心得與意見回饋，持續優化系統功能和使用體驗，提升黑名單共享系統的有效性及實用性。

(三)提供弱點掃描網站之技術諮詢與到點服務

- 將盤點在成大弱掃平台上之受掃描網站，對發現之弱點或已下架網站進行盤點整理，並協助移除已下架網站。亦提供網站修補建議與技術諮詢，並安排到校到點支援服務，強化與下轄學校之連結與技術交流，以提升整體校園網站之安全性與維運能量。

肆、特色服務

請說明貴中心服務推動特色、辦理成效。

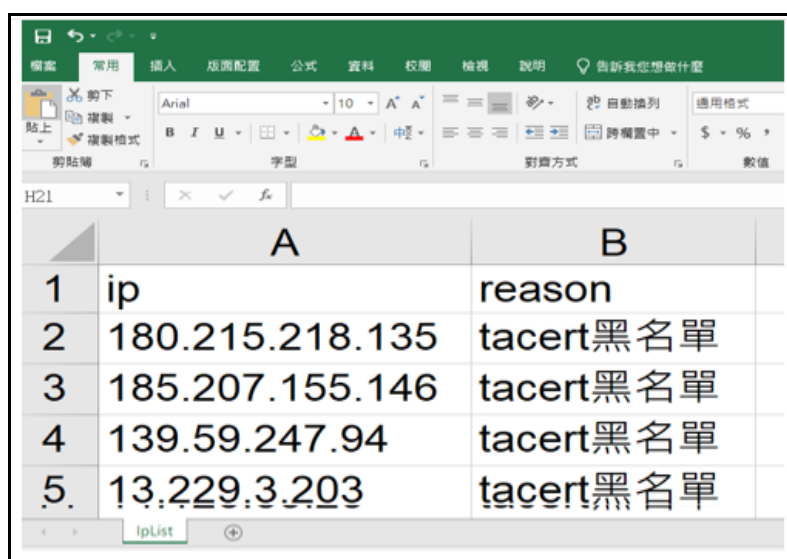
說明：

- 1.114 年度服務特色辦理成效。
- 2.115 年未來創新服務目標與營運計畫。
- 3.創新特色議題(對 TANet 網路或資安管理有助益之特色服務)。
- 4.其他專案服務(教育部或其他機關補助或計畫專案之服務規劃或成果，無則免填)。

一、114 年度服務特色辦理成效。

(一)黑名單系統

1. 黑名單系統-首頁：<https://blacklist.kpprc.edu.tw/login>
2. 黑名單系統-上傳檔案



	A	B
1	ip	reason
2	180.215.218.135	tacert黑名單
3	185.207.155.146	tacert黑名單
4	139.59.247.94	tacert黑名單
5	13.229.3.203	tacert黑名單

3. 黑名單系統-黑名單管理

blacklist.kpprc.edu.tw/not-checked-out-blacklists

Zimbra 網頁用戶端...tanwpmas2 - Synol...研究計畫助理IPS中山大學 人員查詢CYBERSEC 2023 重...黑名單網站研習後援上海聯勤...中山大學SSO單...觀點博樓網站EV5...

我的上傳檔案我的黑名單黑名單下載上傳檔案管理黑名單管理使用者管理管理書

登入個人檔案登出

黑名單系統

✓ 補救勾選的黑名單

✗ 拒絕勾選的黑名單

Search

X

🔍

☰

↻

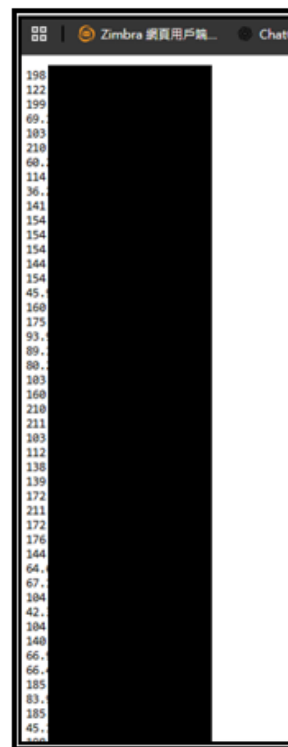
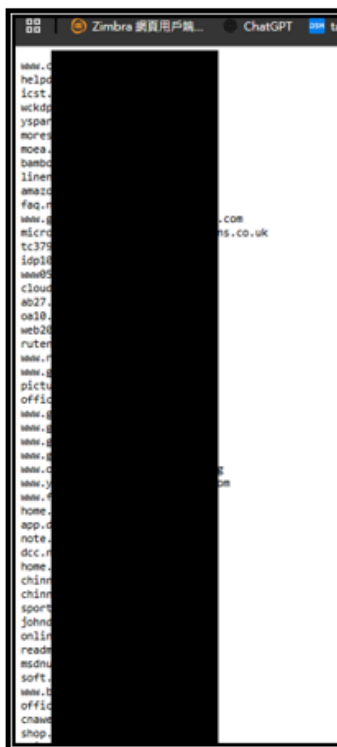
☐	黑名單 IP Filter by 黑名單 IP X	被列入黑名單的原因 Filter by 被列入黑名單的原因 X	創建時間	更新時間	執行
☐	156.248.153.155	tacnet黑名單	2023-10-25 10:46:30	2023-10-25 10:46:30	✓ 通過 ✗ 拒絕
☐	156.248.153.171	tacnet黑名單	2023-10-25 10:46:30	2023-10-25 10:46:30	✓ 通過 ✗ 拒絕
☐	118.107.45.185	tacnet黑名單	2023-10-25 10:46:30	2023-10-25 10:46:30	✓ 通過 ✗ 拒絕
☐	118.107.45.184	tacnet黑名單	2023-10-25 10:46:30	2023-10-25 10:46:30	✓ 通過 ✗ 拒絕
☐	118.107.45.187	tacnet黑名單	2023-10-25 10:46:30	2023-10-25 10:46:30	✓ 通過 ✗ 拒絕
☐	118.107.45.188	tacnet黑名單	2023-10-25 10:46:30	2023-10-25 10:46:30	✓ 通過 ✗ 拒絕
☐	118.107.45.183	tacnet黑名單	2023-10-25 10:46:30	2023-10-25 10:46:30	✓ 通過 ✗ 拒絕
☐	118.107.45.190	tacnet黑名單	2023-10-25 10:46:30	2023-10-25 10:46:30	✓ 通過 ✗ 拒絕
☐	118.194.254.32	tacnet黑名單	2023-10-25 10:46:30	2023-10-25 10:46:30	✓ 通過 ✗ 拒絕
☐	118.107.45.182	tacnet黑名單	2023-10-25 10:46:30	2023-10-25 10:46:30	✓ 通過 ✗ 拒絕

Rows per page 101-10 of 130<< >>

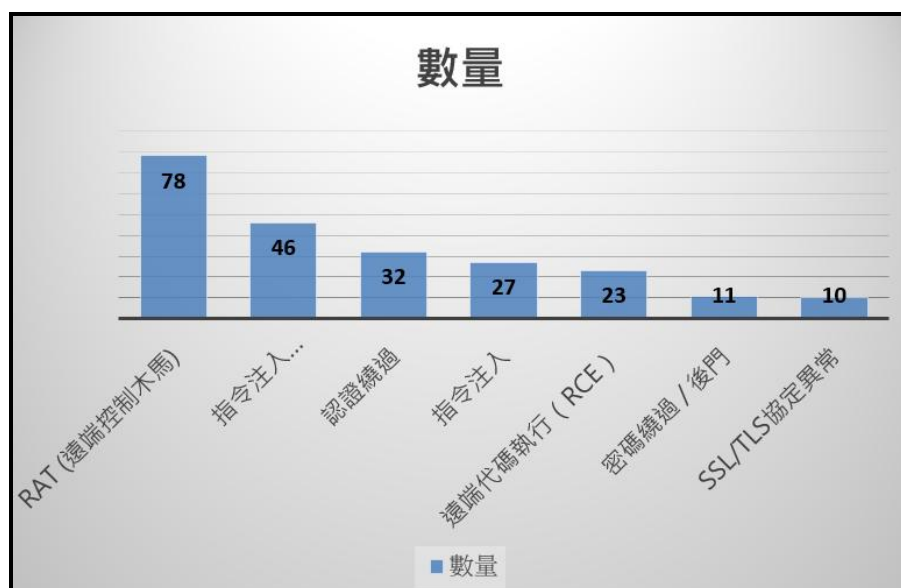
4. 黑名單系統-教育部惡意網域、IP 引用

教育部惡意網域黑名單

教育部惡意IP黑名單



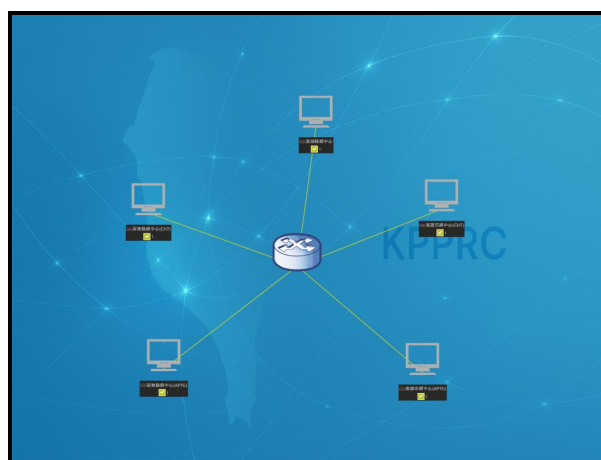
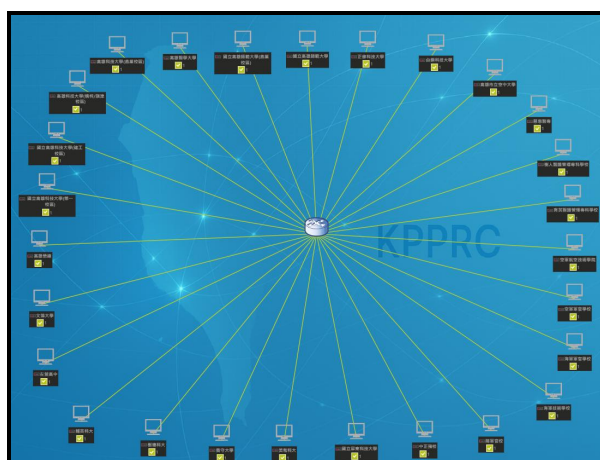
5. 黑名單系統-黑名單共享



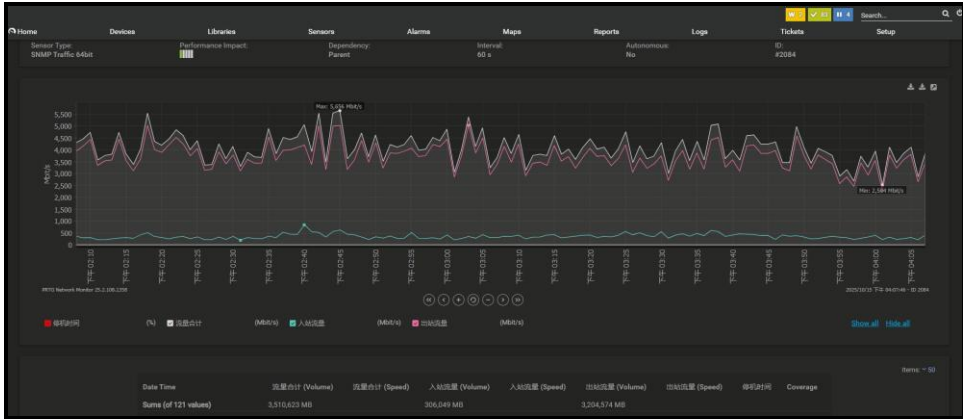
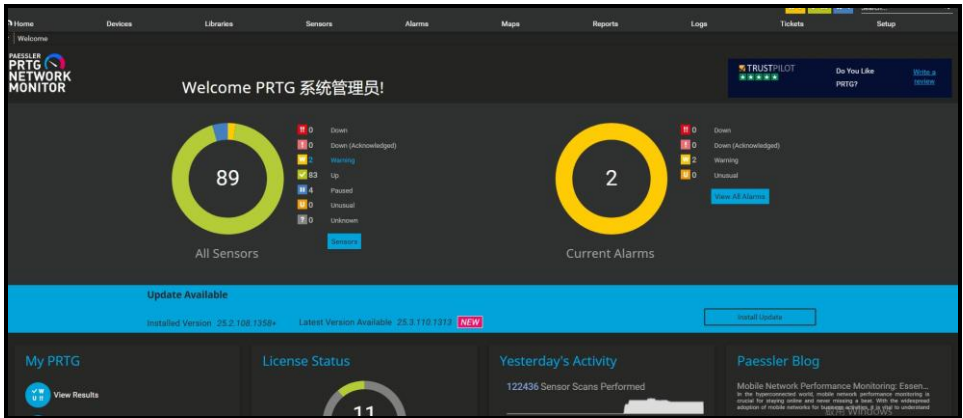
#	特徵名稱	攻擊對象/漏洞	攻擊類型	風險等級	說明	建議處理
1	BO_CLIENT_TRAFFIC_DETECT	受感染電腦	RAT (遠端控制木馬)	高	偵測到主機嘗試連線到疑似 Back Orifice 控制端	調查內部 IP，掃描惡意軟體，封鎖目的 IP
2	SERVER-OTHER RealTek UDP Server command injection attempt	Realtek 裝置	指令注入 (Command Injection)	高	攻擊者透過 UDP 封包執行任意指令，常針對 IoT	封鎖來源 IP，檢查是否有 Realtek 裝置暴露
3	SERVER-OTHER Fortinet FortiOS and FortiProxy authentication bypass attempt	Fortinet 防火牆設備	認證繞過	高	試圖繞過 Fortinet 的登入驗證，可能為 CVE 漏洞攻擊	更新 Fortinet 韌體、封鎖來源 IP
4	Zyxel.Firmware.error.message.Command.Injection	Zyxel 設備	指令注入	高	漏洞利用錯誤回應訊息執行惡意指令	封鎖來源 IP、檢查 Zyxel 韌體版本
5	SERVER-WEBAPP PHP PHP-CGI command execution attempt	PHP-CGI Web 伺服器	遠端代碼執行 (RCE)	高	PHP-CGI 的漏洞可讓攻擊者遠端執行命令	更新 PHP、封鎖攻擊者 IP
6	Netcore.Netis.Devices.Hardcoded.Password.Security.Bypass	Netis 路由器	密碼繞過 / 後門	中~高	利用內建密碼登入管理介面，無需驗證	升級設備、封鎖來源 IP
7	SSL_INVALID_CLIENT_HELLO	任意 HTTPS 客戶端	SSL/TLS協定異常	中	收到不合法的 Client Hello 封包，可能為掃描或弱加密工具	留意是否為掃描工具，可記錄封包源頭觀察

(二)建置新的網路流量監控軟體(PRTG)

1. PRTG 流量監控：提供下轄學校即時監控斷線網路圖。



2. PRTG 流量監控：提供詳細設備狀況、流量、延遲及掉包狀況。

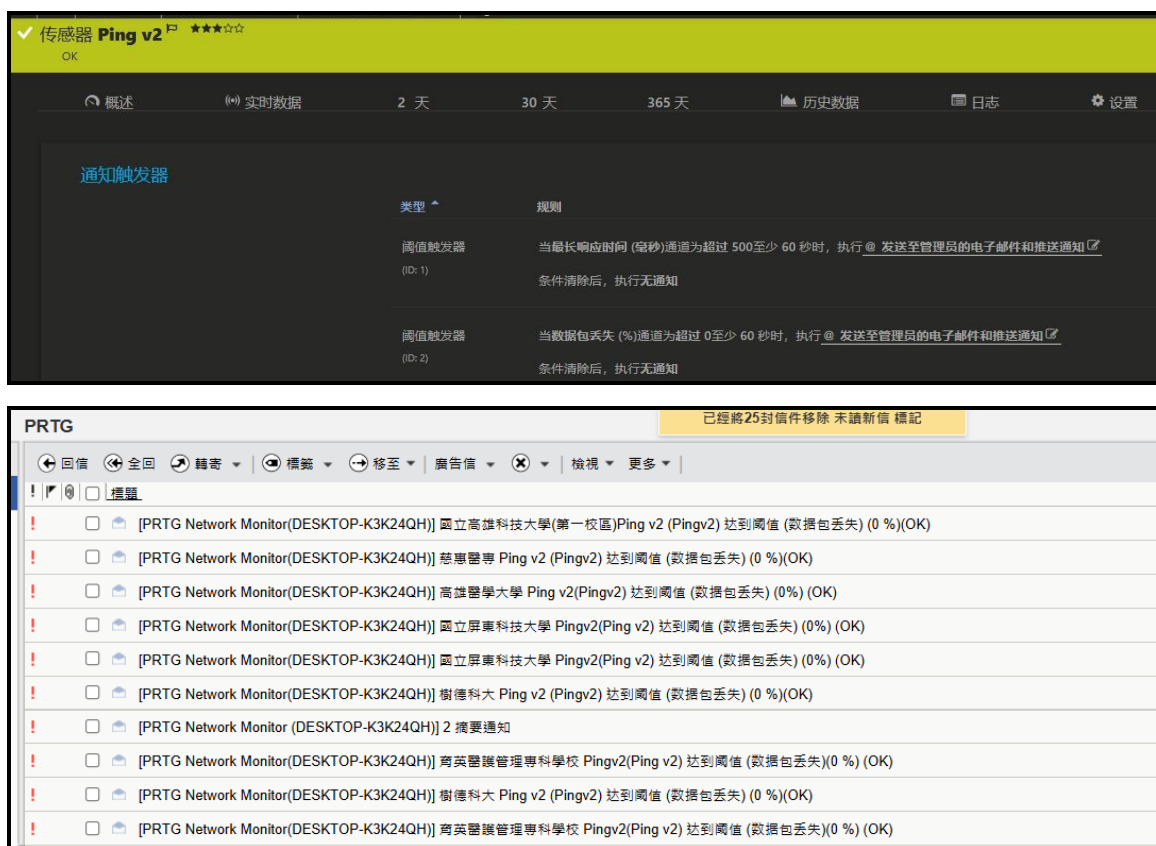


Date Time	流量合计 (Volume)	流量合计 (Speed)	入站流量 (Volume)	入站流量 (Speed)	出站流量 (Volume)	出站流量 (Speed)	停机时间	Coverage
Sums (of 120 values)	3,474,172 MB		307,580 MB		3,166,592 MB			
Averages (of 120 values)	28,951 MB	4,048 Mbit/s	2,563 MB	358 Mbit/s	26,388 MB	3,690 Mbit/s	0 %	100 %

Date Time ^	流量合计 (Volume) ▾	流量合计 (Speed) ▾	入站流量 (Volume) ▾	入站流量 (Speed) ▾	出站流量 (Volume) ▾	出站流量 (Speed) ▾	停机时间 ▾	Coverage ▾
2025/10/15 下午 04:16:29	22,152 MB	3,101 Mbit/s	2,005 MB	281 Mbit/s	20,147 MB	2,820 Mbit/s	0 %	100 %
2025/10/15 下午 04:15:29	30,349 MB	4,238 Mbit/s	2,810 MB	392 Mbit/s	27,539 MB	3,846 Mbit/s	0 %	100 %
2025/10/15 下午 04:14:29	25,900 MB	3,626 Mbit/s	2,307 MB	323 Mbit/s	23,593 MB	3,303 Mbit/s	0 %	100 %
2025/10/15 下午 04:13:29	31,830 MB	4,445 Mbit/s	2,866 MB	400 Mbit/s	28,964 MB	4,045 Mbit/s	0 %	100 %
2025/10/15 下午 04:12:29	26,230 MB	3,668 Mbit/s	2,456 MB	343 Mbit/s	23,774 MB	3,324 Mbit/s	0 %	100 %
2025/10/15 下午 04:11:29	22,568 MB	3,241 Mbit/s	1,901 MB	273 Mbit/s	20,667 MB	2,968 Mbit/s	0 %	100 %
2025/10/15 下午 04:10:30	33,582 MB	4,575 Mbit/s	2,588 MB	353 Mbit/s	30,994 MB	4,223 Mbit/s	0 %	100 %
2025/10/15 下午 04:09:29	24,596 MB	3,439 Mbit/s	2,082 MB	291 Mbit/s	22,514 MB	3,148 Mbit/s	0 %	100 %
2025/10/15 下午 04:08:29	36,249 MB	5,069 Mbit/s	2,709 MB	379 Mbit/s	33,541 MB	4,690 Mbit/s	0 %	100 %
2025/10/15 下午 04:07:29	27,551 MB	3,852 Mbit/s	2,901 MB	406 Mbit/s	24,650 MB	3,446 Mbit/s	0 %	100 %

Date Time ^	响应时间 ▾	状态 (Reachable) ▾	最短响应时间 ▾	最长响应时间 ▾	数据包丢失 ▾	停机时间 ▾	Coverage ▾
2025/10/15 下午 04:19:06	0 msec	Reachable	0 msec	1 msec	0 %	0 %	100 %
2025/10/15 下午 04:18:06	1 msec	Reachable	0 msec	1 msec	0 %	0 %	100 %
2025/10/15 下午 04:17:06	2 msec	Reachable	0 msec	3 msec	0 %	0 %	100 %
2025/10/15 下午 04:16:06	1 msec	Reachable	0 msec	1 msec	0 %	0 %	100 %
2025/10/15 下午 04:15:06	1 msec	Reachable	0 msec	1 msec	0 %	0 %	100 %
2025/10/15 下午 04:14:06	1 msec	Reachable	1 msec	1 msec	0 %	0 %	100 %
2025/10/15 下午 04:13:06	2 msec	Reachable	1 msec	2 msec	0 %	0 %	100 %
2025/10/15 下午 04:12:06	0 msec	Reachable	0 msec	1 msec	0 %	0 %	100 %
2025/10/15 下午 04:11:06	0 msec	Reachable	0 msec	1 msec	0 %	0 %	100 %
2025/10/15 下午 04:10:06	1 msec	Reachable	0 msec	1 msec	0 %	0 %	100 %
2025/10/15 下午 04:09:06	1 msec	Reachable	0 msec	1 msec	0 %	0 %	100 %
2025/10/15 下午 04:08:06	0 msec	Reachable	0 msec	1 msec	0 %	0 %	100 %
2025/10/15 下午 04:07:06	0 msec	Reachable	0 msec	2 msec	0 %	0 %	100 %

3. PRTG 流量監控：透過 PRTG 建立網路流量監控機制，設定延遲與中斷警示門檻，能在異常發生的第一時間即時通知管理人員，確保問題能迅速被發現與處理。



二、115 年未來創新服務目標與營運計畫。

(一)更掌握 PRTG 流量監控軟體服務

- 持續深化對 PRTG 監控系統的運用，提供更多元的監控服務項目，如流量異常告警、延遲與中斷監測、頻寬使用分析等，協助即時掌握網路狀況，提升整體監控效能與維運品質。

(二)持續加強與下轄學校之技術交流與實地支援

- 主動聯繫下轄學校，了解其網路環境與技術需求，並依實際狀況提供客製化的技術服務與諮詢支援，確保問題能即時解決，強化整體網路運作效率與合作關係。

(三)提供更多元的教育訓練主題

- 持續規劃並提供多元化的教育訓練課程與主題，強化下轄學校在資安防護與網路管理等面向的專業能力，提升整體技術素養與應變能力。

三、創新特色議題(對 TANet 網路或資安管理有助益之特色服務)。

(一)精進網路裝置監測服務系統。

(二)協助連線單位有關 TANet 連線及資安相關問題排除

(三)持續推動區網中心與連線單位夥伴技術分享與工具使用及提供。

(四)持續推動新增完善黑名單系統，更新系統版本、漏洞修補、普及使用。

四、其他專案服務(教育部或其他機關補助或計畫專案之服務規劃或成果，無則免填)。

(一)TANet 青少年網路內容防護

- 1.簡介：高屏澎區網中心自行開發之不當資訊防護系統，以防護全國各區縣市網路中心青少年存取不適合網站，並將核心技術深留於學術網路中。
- 2.說明：
 - (1) 已導入 12 個區網中心及下轄 22 個縣市教育網路中心，防護範圍涵蓋全國。
 - (2) 持續強化技術、改善報表系統呈現方式，並與相關單位建立合作關係。
 - (3) 研發 AI 生成黑名單功能、結合各作業系統替代 NGA 之防護軟體。



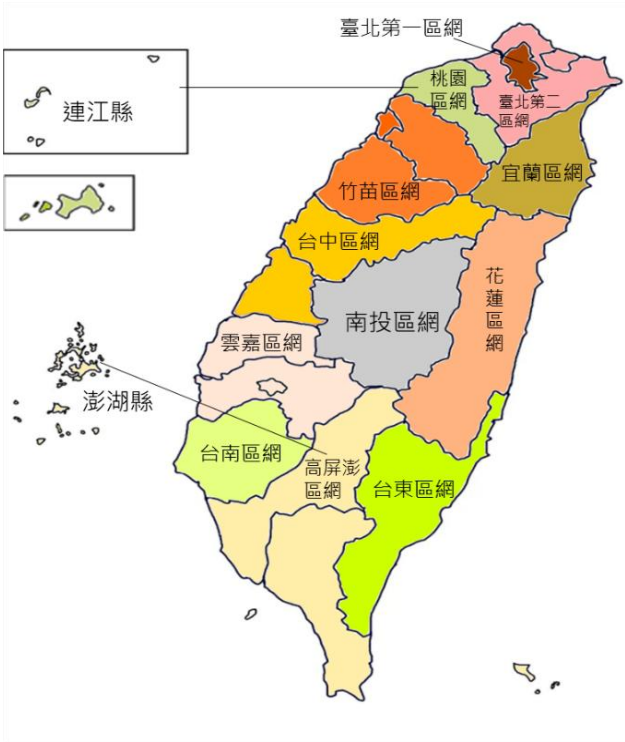
**系統研發與維運
UI介面改善**
防護技術研發與維運、維護資料庫系統、改善報表系統UI介面、建置防護系統資訊首頁。



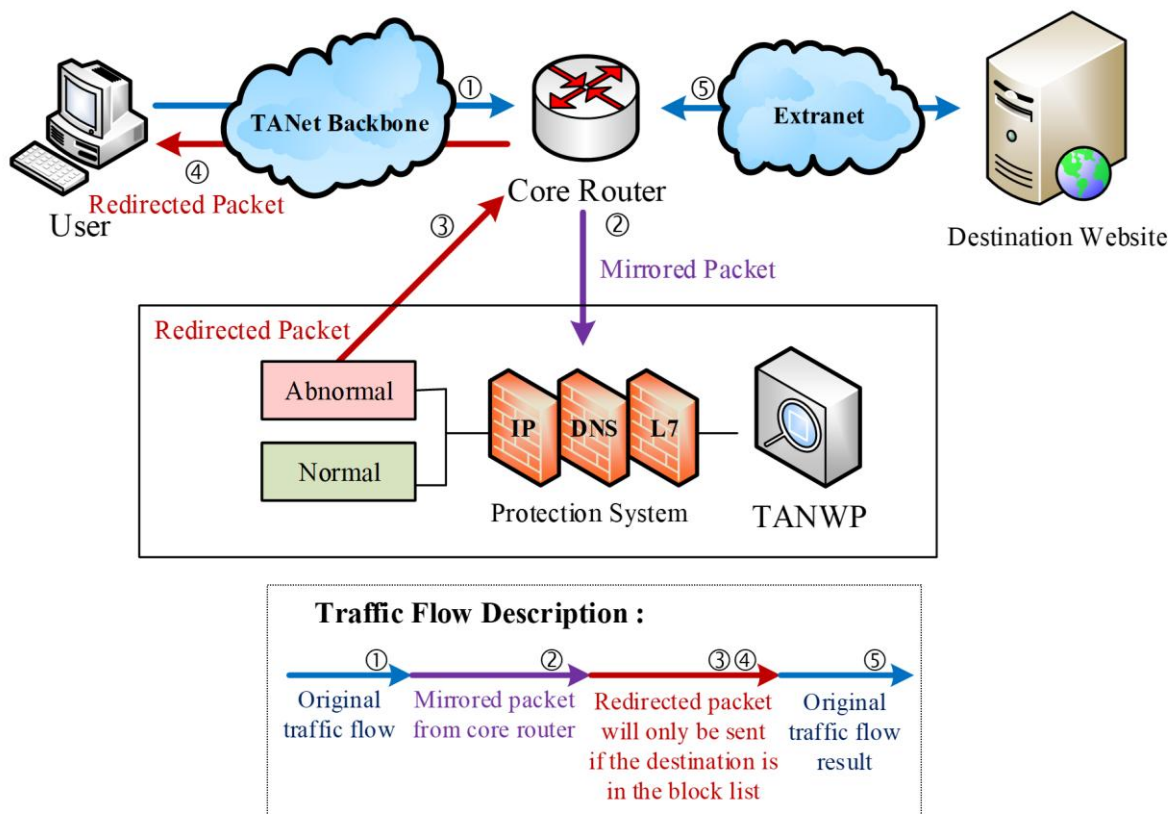
**研發AI生成黑名單
替代NGA防護軟體**
開發AI生成黑名單機制識別潛在不當資訊網站，並提供替代NGA之防護軟體及操作方式。



**防護範圍
涵蓋全國**
已導入12個區網中心及轄下22個縣市教育網路中心，防護範圍涵蓋全國。



3.防護架構：過濾防護範圍內 HTTP 或 HTTPS 網頁連線封包，透過 IP、DNS、Layer7 三重防護機制比對資料庫，若為黑名單網站則發送阻擋封包（DNS Response & HTTP Injection）讓使用者頁面重新導向特定網頁。



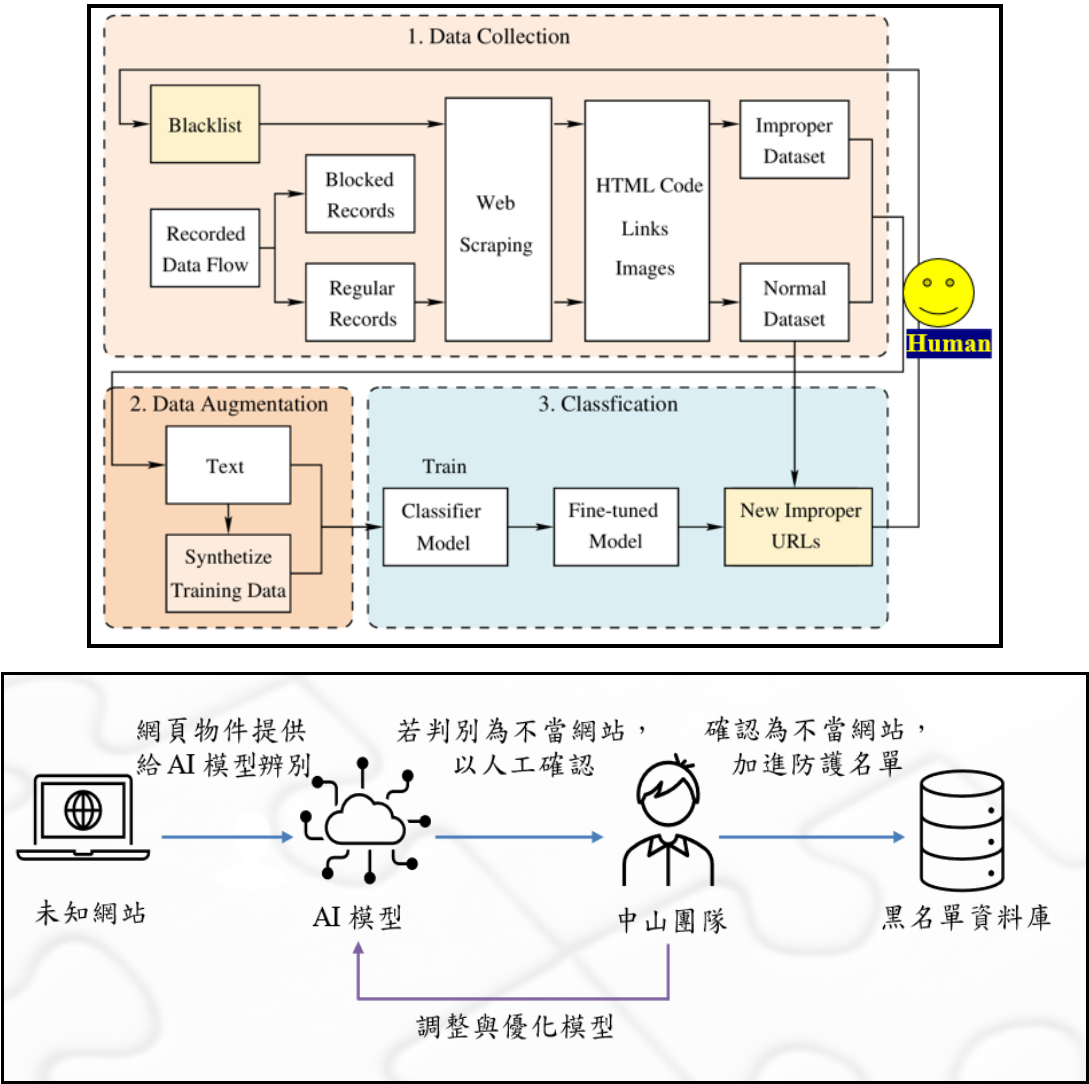
4.TANet 青少年網路內容防護成效—114 年防護成效統計表：

區域	縣市	114年1月至9月		
		瀏覽次數	阻擋次數	阻擋比率
高屏澎區網	高雄市網	36,411,770,549	285,567,018	0.78%
	屏東縣網	12,685,494,962	1,147,442,720	9.05%
	澎湖縣網	3,243,374,317	7,903,740	0.24%
	高屏澎區網高中職	188,919,790	221,531	0.12%
	高屏澎區網全部	52,529,559,618	1,441,135,009	2.74%

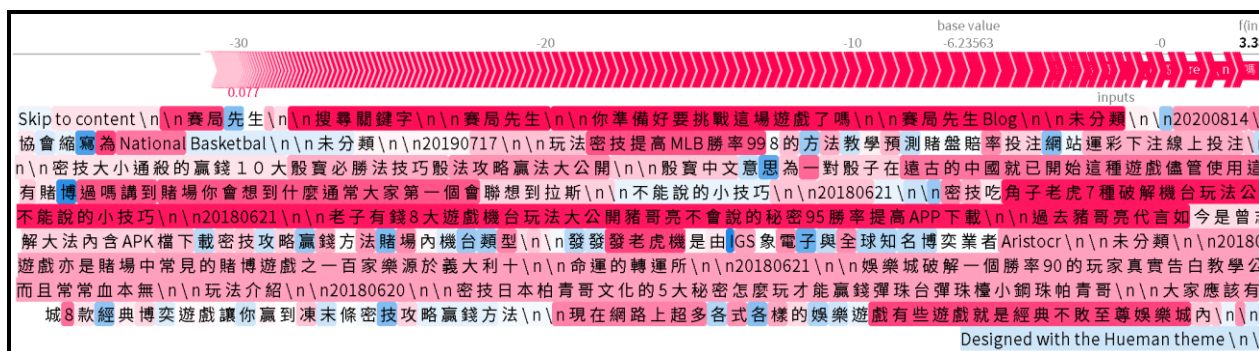
5.設計與發展不當資訊呈現之數位儀表板：



6.以 AI 系統半自動化產生不當網站黑名單：



- 以 SHAP (SHapley Additive exPlanations) 嘗試了解與賭博類別相關內容：賭博網頁



- 為提供使用者快速測試其網路環境是否在防護範圍內，團隊建置阻擋測試網頁，在瀏覽器中輸入測試網址即可確認。
- 阻擋測試網址：<https://pcheck.kpprc.edu.tw/>



- 若在學術網路連線中發現未被阻擋的不當資訊網站或可能被誤擋的具教學性質之網站，可至 TANWP 官網進行申訴檢舉。
- 申訴檢舉網址：<https://tanwp.kpprc.edu.tw/feedback/>

TANWP

申訴檢舉

回報種類 *

☒ 回報不當網站
 ☐ 回報網站誤擋

姓名 *

例：王大明。

服務單位 *

例：○○國小、○○國中、○○縣/市教育局...等。

職稱 *

例：老師、組長、主任、管理師...等。

聯絡信箱 *

例：john@doe.com。

回報網址列表 *

回報原因 *

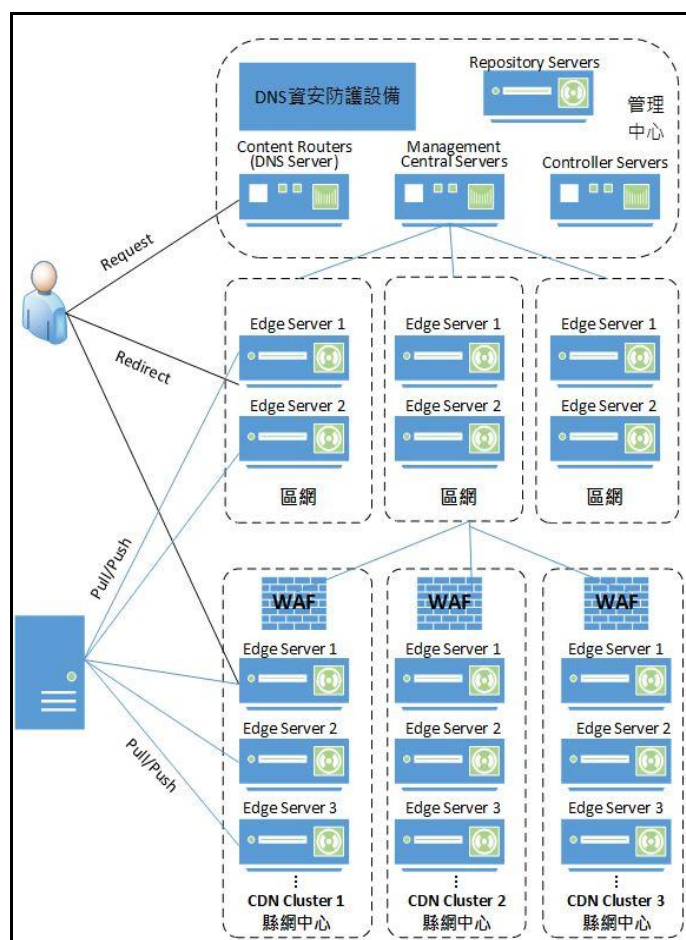
(二)TANet 內容傳遞網路計畫(CDN)

1.計畫概述：

- TANet CDN (Content Delivery Network, CDN)以本地內容傳遞路由服務伺服器（LCDRS）內建域名解析及內容派發功能，有效使師生能就近快速取得數位學習資源，離島學校也能透過在地節點快速獲取學習資源，大幅縮短到臺灣本島的網路傳遞時間，實現「數位學習零距離」的目標。
- 教育部於全國 22 縣市教育網路中心及 13 區域網路中心部署 TANet CDN 節點，透過站點串聯強化安全性及可用性，擴大內容傳遞網路的服務範圍。
- 各 CDN 節點皆擇定 Edge Server 安裝 LCDRS 服務，兼具 DNS resolver 及派發系統功能，並內建教育部（含 TWNIC）及不當資訊 RPZ 清單。



2. 系統架構：



3. TANet CDN 服務網

- 本計畫設置服務網站提供電子佈告欄、CDN 服務目標及功能介紹，並提供網站申請服務流程，讓有意願申請 CDN 服務單位進行諮詢及資訊取得。

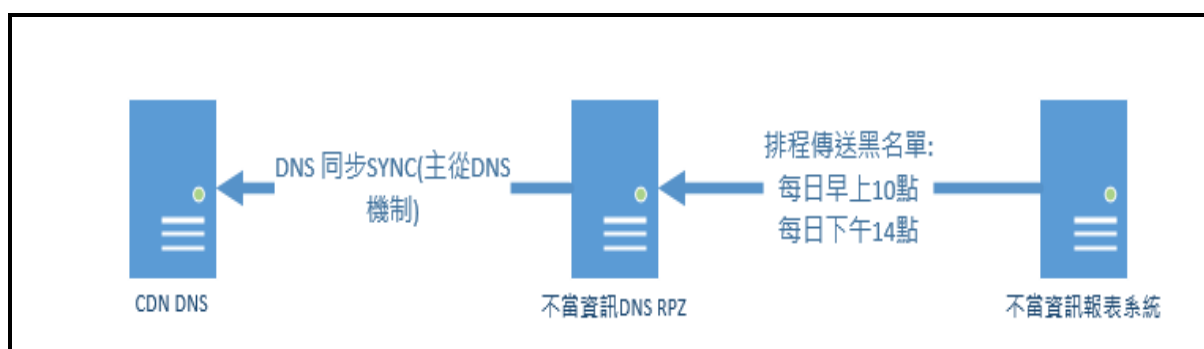


- 教育部持續推廣相關教育資源網站加入 TANet CDN 服務，已涵蓋 37 個不同領域教育資源網站，提

供全國校園師生更優質順暢的學術網路環境。

網站名稱	網站URL	網站名稱	網站URL
教育部全球資訊網	www.edu.tw	國字標準字體筆順學習網	stroke-order.learningweb.moe.edu.tw
	www.moe.gov.tw	全國語文競賽網	nlc.moe.edu.tw
	ws.moe.edu.tw	美感教育資源整合平臺	aew.moe.edu.tw
	dept.moe.gov.tw	臺灣台語常用詞辭典	sutian.moe.edu.tw
因材網	adl.edu.tw	教育部美感與設計課程創新計畫網站	aade.project.edu.tw
愛學網(影音專區)	stv.naer.edu.tw	藝秀臺	artshow.edu.tw
	stvstreaming.naer.edu.tw	國民小學師資資源科學科知能評量網站	tl-assessment.edu.tw
教育大市集	market.cloud.edu.tw	台灣客語拼音學習網	happyhakka.moe.edu.tw
教育暨數位學習入口網(數位媒體影音)	cloud.edu.tw	臺灣客語辭典	hakkadict.moe.edu.tw
	media.video.cloud.edu.tw	臺灣台語羅馬字拼音教學網	tailo.moe.edu.tw
臺灣台語動畫網	twbanga.moe.edu.tw	學科術語臺灣台語及臺灣客語對譯查詢	stti.moe.edu.tw
推動中小學數位學習精進方案入口網	pads.moe.edu.tw	中小學資訊素養與認知網站	eliteracy.edu.tw
共構式計畫網站暨成果	proj.moe.edu.tw	教育部防災教育資訊網	disaster.moe.edu.tw
TANet 無線網路漫遊交換中心	roamingcenter.ndhu.edu.tw	本土語言資源網	mhi.moe.edu.tw
臺東縣雲端社群播客系統	igt.boe.ttct.edu.tw	偏鄉數位培力推動計畫	itaiwan.moe.gov.tw
屏東縣本土語言資源網	www.lgps.ptc.edu.tw	MUSE 大玩家	muse.moe.gov.tw
宜蘭 Scratch 3	s3.ilc.edu.tw	教育部媒體素養教育資源網	mlearn.moe.gov.tw
TANet CDN 服務網	www.tanetcdn.edu.tw	教育百科	pedia.cloud.edu.tw
教育部不當資訊防護系統	tanwp-bk.kpprc.edu.tw	(計37個代管網站)	

- 不當資訊 DNS RPZ 同步機制：透過 RPZ (Response Policy Zone)協定分享阻擋黑名單給 CDN 系統，預計導入 22 縣市教育網路中心及 13 區域網路中心的 Local CDRS (CDN DNS 服務)。
- 不當資訊報表系統每日會依照預設排程，自動在上午 10 點及下午 14 點進行黑名單同步作業，將最新的阻擋黑名單提供給 CDN 計畫進行測試。



伍、前(113)年度執行成效評量改進意見項目成效精進情形

1. 資安事件通報審核平均時數為 2.91 小時，高於其他區網時間，建議說明原因，同時可研擬如何降低審核時間。

- 精進說明：謝謝委員建議，因審核人員僅一人，常因設備問題外出維修，不在電腦前，無法及時審核，今年已聘到另一名資安人員，有及時審核，效果會有明顯改善。

2. 區網管理會辦理 2 次，出席率分別為 75%及 72%，建議仍應提升會議出席率。

- 精進說明：謝謝委員建議，會再去電詢問連線單位未出席原因及如何改善。

3. 目前經費是否足夠？未來如經費減少或暫時凍結時，建議學校預為適度規劃，且若有人員異動時，建議可規劃完善交接，並針對人員空窗期適度因應。

- 精進說明：謝謝委員建議，有陸續針對工作上遇到的問題建立教學文件及技術文件整理，

還有異常連線紀錄及排除方式，以利有適當的 SOP。

4. 本區網已經維運多年，特色服務為何？有無創新的精進措施或規劃？

➤精進說明：謝謝委員建議，因人力與經驗暫且不足，未來會加強人員專業訓練，並朝加強與下轄學校交流與實地輔導為主。

5. 對區網中心之網管、資安及雲端人力的服務績效未有相關具體內容，另區網中心人力運作人數一致性，請再確認。

➤精進說明：謝謝委員建議，會再重新計算區網維運人力。

6. 對所描述之 114 年目標與 113 辦理情形相似，建議再構思。

➤精進說明：謝謝委員建議，會再重新構思目前狀況可提供的技術與服務。

7. 因高屏澎服務之縣市網路中心的連線地區，是否有因應地服務或使用需求給予適當的協助，建議可將蒐集的相關問題規劃對應的協助作業。

➤精進說明：謝謝委員建議，會再加強外島交流，關心並提升外島服務與連結。

8. 對連線單位異常反應處理，建議能補充處理時效的說明。

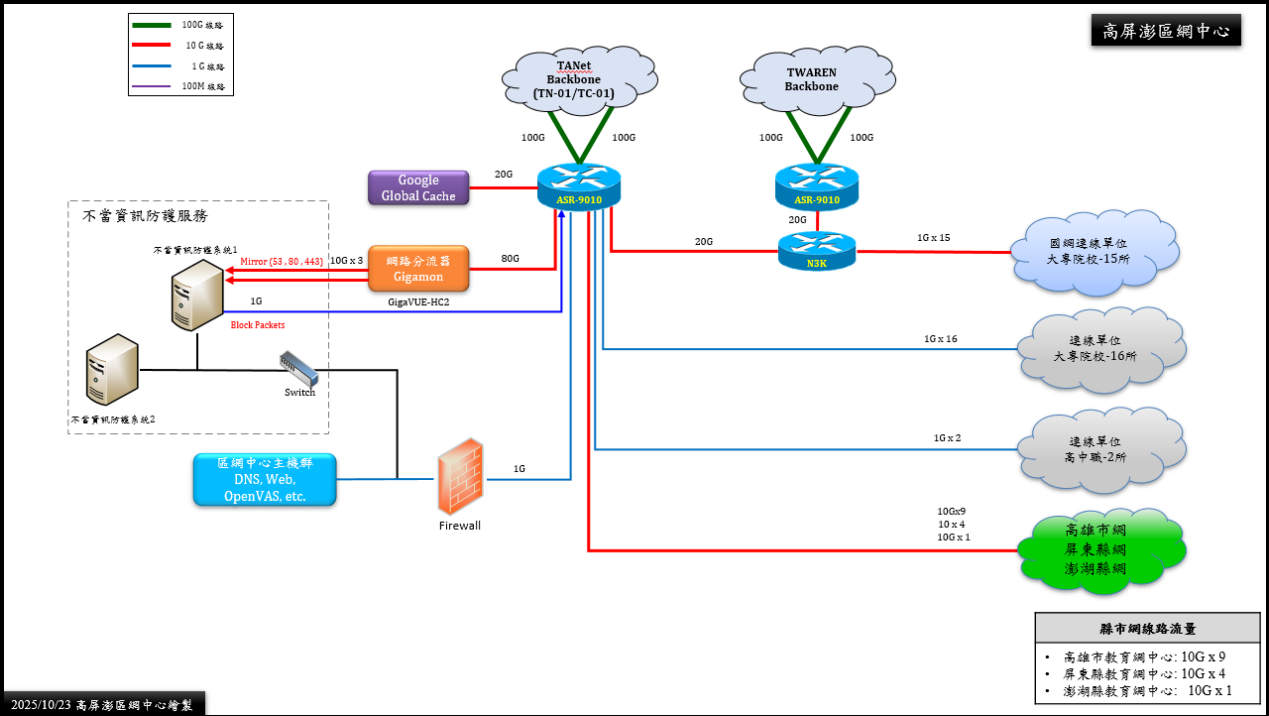
➤精進說明：謝謝委員建議，會詳細記錄每次處理異常連線日期及時間並歸檔，之後會補充詳細時間。

9. 連線學校的清單有部分學校已退場或更名，建議再檢視。

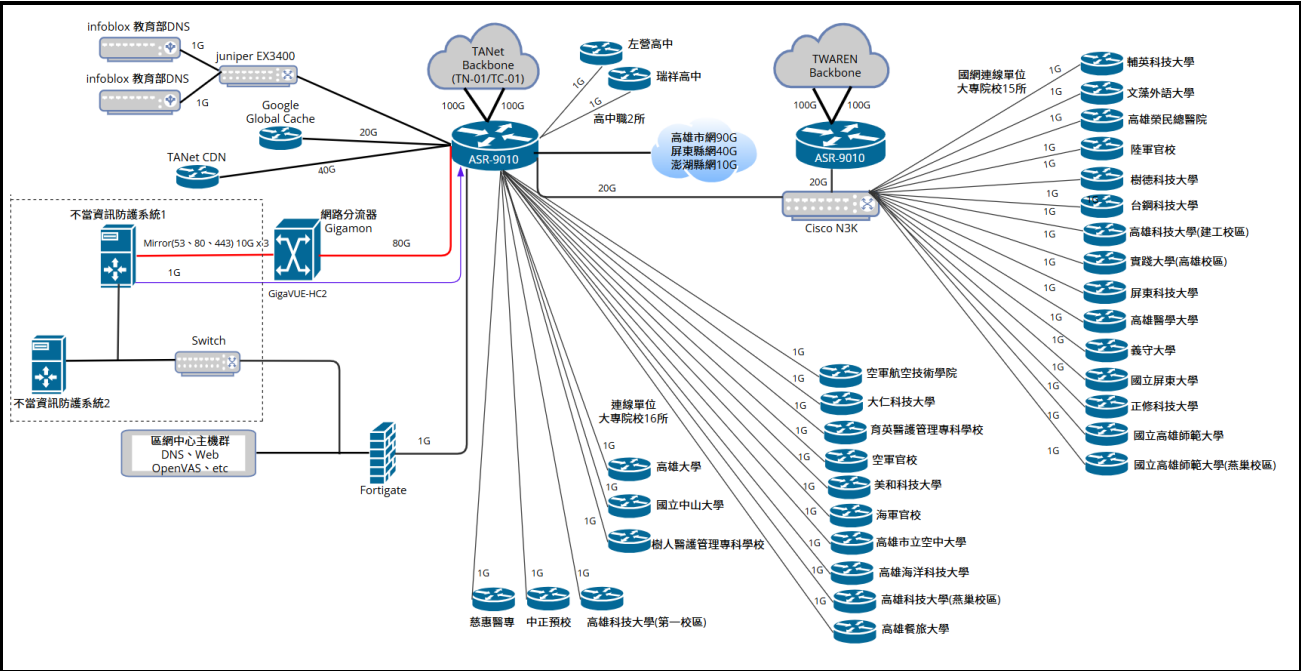
➤精進說明：謝謝委員建議，會再安排時間盤點與更新下轄學校資訊。

附表 1：區網網路架構圖

一、區網與連線單位(含縣(市)教育網路、連線學校、其他連線單位等)、TANet、Internet(Peering)的總體架構圖



二、網路配合各種應用架構(如連線分流、頻寬管理)或資安架構(防火牆、IDS/IPS/WAF)的規劃或實際運作架構



附表 2：連線資訊詳細表

1.請以電路服務商分列填寫，若單位/學校有多條連線但為同一供應商，請填寫一列合計頻寬，若有多供應商之連線，每一供應商填寫一列，寫多列個別填寫多列。

2.表格可自行調整。

		單位/學校名稱	電路頻寬(合計)	電路服務商	備註
縣(市)教育網中心	1.	高雄市教網中心	50G	中華電信	5 路 10G 介面
	2.	高雄市教網中心	40G	遠傳電信	4 路 10G 介面
	3.	屏東縣網中心	20G	中華電信	2 路 10G 介面
	4.	屏東縣網中心	20G	遠傳電信	2 路 10G 介面
	5.	澎湖縣網中心	5G	中華電信	1 路 10G 介面
大專校院	1.	高雄市立空中大學	1G	中華電信	單 1G 介面
	2.	私立慈惠醫專	500M	中華電信	單 1G 介面
	3.	私立樹人醫專	400M	中華電信	單 1G 介面
	4.	國立中山大學	10G	中華電信	單 10G 介面
	5.	國立澎湖科技大學	500M	中華電信	接在澎湖縣網下
	6.	中正國防幹部預備學校	1G	中華電信	單 1G 介面
	7.	空軍軍官學校	1G	遠傳電信	單 1G 介面
	8.	空軍航空技術學院	1G	中華電信	單 1G 介面
	9.	海軍軍官學校	400M	中華電信	單 1G 介面
	10.	陸軍軍官學校	1G	遠傳電信	單 1G 介面
	11.	國立高雄大學	600M	中華電信	單 1G 介面
	12.	國立高雄師範大學和平校區	1G	中華電信	單 1G 介面
	13.	國立高雄師範大學燕巢校區	1G	中華電信	單 1G 介面
	14.	國立高雄科技大學第一校區	1G	中華電信	單 1G 介面
	15.	國立高雄科技大學楠梓校區	1G	中華電信	單 1G 介面
	16.	國立高雄科技大學建工校區	1G	中華電信	單 1G 介面
	17.	國立高雄科技大學旗津校區	1G	中華電信	單 1G 介面
	18.	國立高雄餐旅大學	1G	中華電信	單 1G 介面
	19.	私立文藻外語大學	1G	遠傳電信	單 1G 介面
	20.	私立正修科技大學	10G	中華電信	單 10G 介面
	21.	私立育英護理專科學校	500M	遠傳電信	單 1G 介面
	22.	私立高雄醫學大學	1G	中華電信	單 1G 介面
	23.	私立義守大學	1G	中華電信	單 1G 介面
	24.	私立實踐大學高雄校區	1G	中華電信	單 1G 介面
	25.	私立輔英科技大學	1G	中華電信	單 1G 介面
	26.	私立樹德科技大學	1G	中華電信	單 1G 介面
	27.	國立屏東科技大學	1G	中華電信	單 1G 介面

	28.	國立屏東大學	1G	中華電信	單 1G 介面
	29.	私立大仁科技大學	500M	中華電信	單 1G 介面
	30.	私立美和科技大學	200M	台灣大哥大	單 1G 介面
	31.	私立台鋼科技大學	1G	中華電信	單 1G 介面
高中職校	1.	左營高中	300M	中華電信	單 1G 介面
	2.	瑞祥高中	1G	中華電信	單 1G 介面
非學校之 連線單位 (不含 ISP)	1.	高雄榮民總醫院	1G	中華電信	單 1G 介面
連接 TANet	1.	台南主節點	100G		單 100G 介面
	2.	台中主節點	100G		單 100G 介面
其他連線	1.	中華電信	10G		
	2.	新世紀資通	500M		
	3.	新世紀資通	1G		
	4.	台灣固網	1G		
	5.	亞太電信	100M		
	6.	GGC Server	20G		