



114年度高屏澎區網 執行成效報告

國立中山大學圖書與資訊處

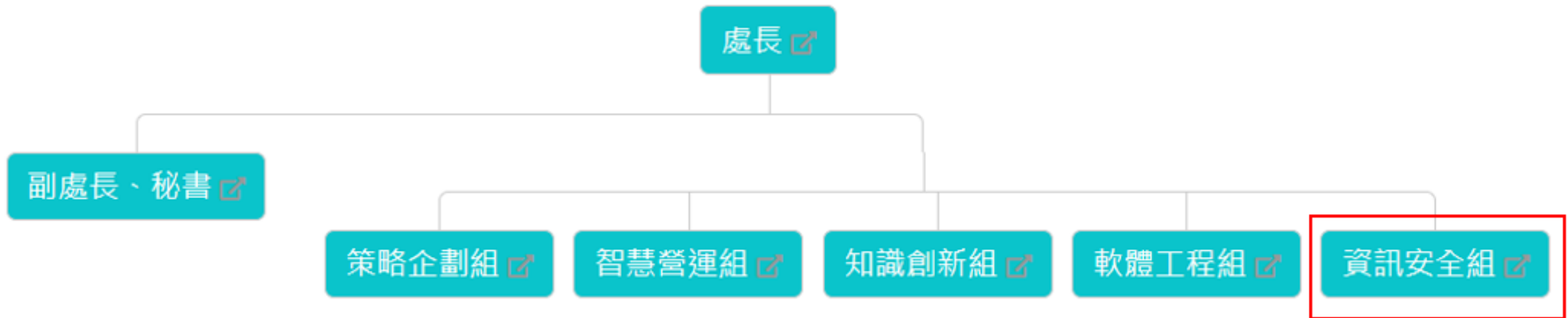
處長：鄺獻榮教授

報告人：蔡崇煒副處長、王聖全組長、佘冠諄組員

報告目錄

1. 高屏澎區網中心人員組成
2. 網路中心基礎維運
3. 網路及資安技術支援
4. 特色服務
5. 連線單位需求分析及滿意度調查
6. 未來營運目標

1.高屏澎區網中心人員組成



高屏澎區網中心成員簡歷及業務職掌

處本部

職稱	姓名	Email	主要業務職掌	分機	職務代理人
處長	鄭獻榮	srkuangATcse.nsysu.edu.tw	規劃、綜理督導執行本處各項業務	2400/ 4340	第一順序：鄭獻榮 第二順序：王美惠 第三順序：蔡崇煒
副處長	蔡崇煒	cwtsaiATcse.nsysu.edu.tw	協助處長規劃、綜理督導執行本處各項業務	2402/ 4368	第一順序：王美惠 第二順序：王聖全

資訊安全組

職稱	姓名	Email	主要業務職掌	分機	職務代理人
組長 兼任圖資處副處長	蔡崇煒	cwtsaiATcse.nsysu.edu.tw	1. 綜理組務 2. 教育部TANet區域網路中心維運計畫督導 3. TWAREN計畫督導 4. 教育部TANet青少年網路內容防護計畫督導 5. 教育部TANet內容傳遞網路建置案計畫督導 6. 資訊安全組各項業務及計畫督導	2510/ 4368	第一順序：王聖全 第二順序：孫繡紋 第三順序：黃貴瑛

高屏澎區網中心成員簡歷及業務職掌

技正	廖先生	yc.liaoATmail.nsysu.edu.tw	1. 全校性資通安全維護業務推動 2. ISMS資訊安全相關業務 3. 深耕計畫資安專章業務 4. TANet內容傳遞網路建置案計畫行政業務執行 5. 電子郵件系統管理及維護 6. 其他交辦事項	2531	第一順序：祝先生 第二順序：洪小姐
技士 (英文窗口)	祝先生	ccchuATmail.nsysu.edu.tw	1. ISMS資訊安全相關業務 2. E-mail技術與服務之規劃與執行 3. G-Suite管理與維護 4. 辦理社交工程演練相關業務 5. 政府組態標準(GCB)及VANS部屬 6. 交辦事項	2522	第一順序：廖先生 第二順序：蘇小姐
技術師	蘇小姐	elenaATmail.nsysu.edu.tw	1. TANet內容傳遞網路建置案計畫行政業務執行 2. 經費核銷業務、採購核銷 3. 組內工讀生聘用及核銷 4. 組內行政業務彙辦 5. 其他交辦事項	2509	第一順序：廖先生 第二順序：洪小姐
高級技術師	張小姐	vj70048ATmail.nsysu.edu.tw	1. TANet青少年網路內容防護計劃行政業務 2. 計畫經費核銷業務 3. 組內各項行政業務彙辦 4. 其他交辦事項	2515	第一順序：陳先生 第二順序：余先生
技術師	洪小姐	lilyhungATmail.nsysu.edu.tw	1. TWAREN GigaPOPs維運與相關業務諮詢 2. ISMS資訊安全相關行政業務 3. APCS辦理及聯絡窗口 4. 中山大學資安事件通報與處理 5. NICT服務維運及日本方聯絡窗口	2514	第一順序：余先生 第二順序：祝先生

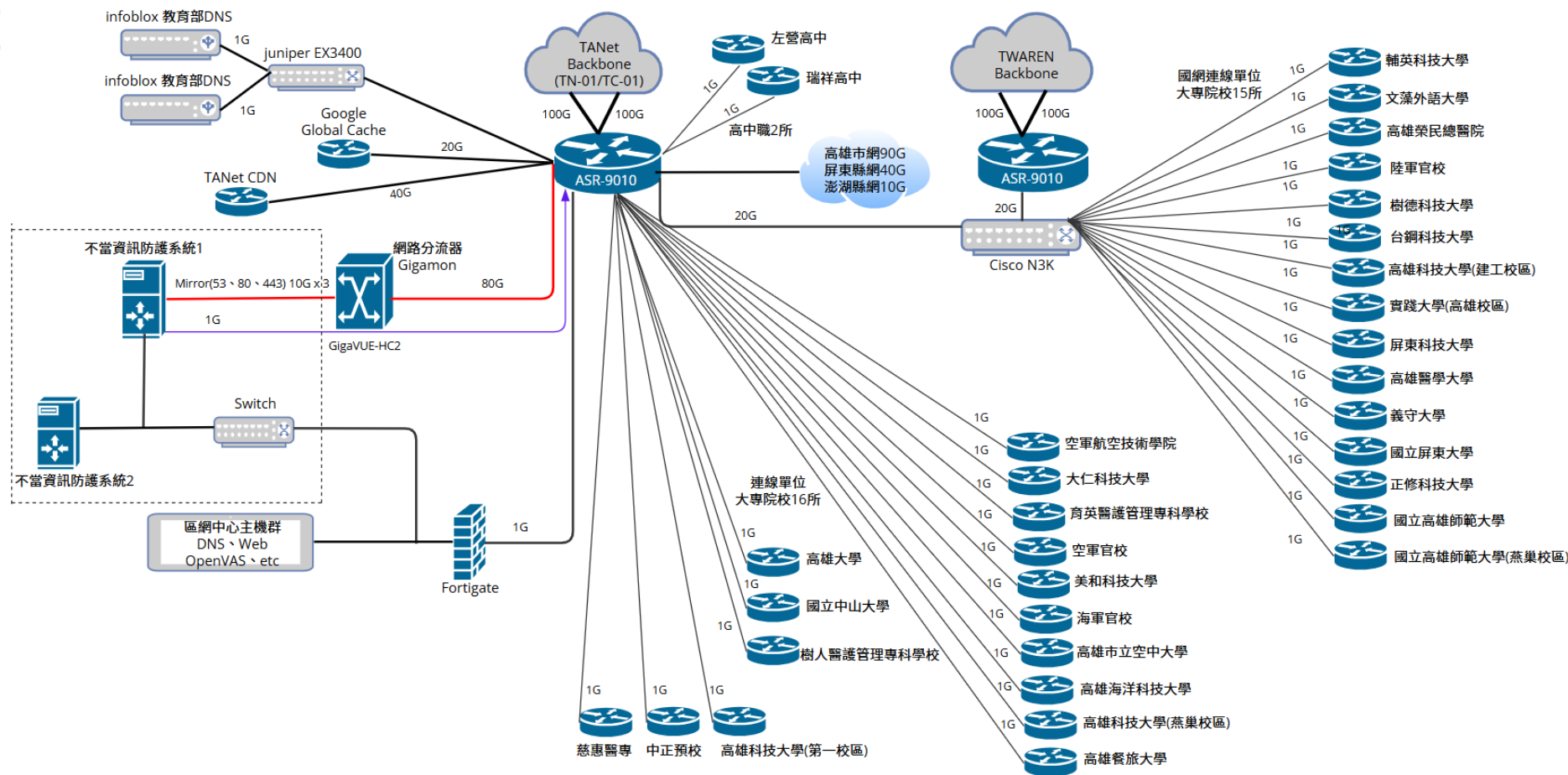
高屏澎區網中心成員簡歷及業務職掌

技術師	洪小姐	lilyhungATmail.nsysu.edu.tw	1. TWAREN GigaPOPs維運與相關業務諮詢 2. ISMS資訊安全相關行政業務 3. APCS辦理及聯絡窗口 4. 中山大學資安事件通報與處理 5. NICT服務維運及日本方聯絡窗口	2514	第一順序：佘先生 第二順序：祝先生
技術師	洪小姐	evahungATmail.nsysu.edu.tw	1. TANet內容傳遞網路建置案計畫行政業務執行 2. 其他交辦事項	2519	第一順序：蘇小姐 第二順序：廖先生
技術師	林小姐	tzslinATmail.nsysu.edu.tw	1. 高屏澎區網中心行政業務執行 2. 其他交辦事項	2509	第一順序：佘先生 第二順序：洪小姐
技術師	佘先生	aaronATmail.nsysu.edu.tw	1. 高屏澎區網計畫執行 2. 高屏澎區網中心相關業務及窗口 3. 教育部DNS Server管理、GGC業務處理 4. 區網中心資安事件通報與處理 5. 校園IPS入侵偵測防禦系統管理 6. 校園與高屏澎區網VOIP主機維護管理 7. 圖資大樓門禁系統管理 8. 區域網路中心管理	2517	第一順序：洪小姐 第二順序：祝先生
高級技術師	陳先生	eric.chenATmail.nsysu.edu.tw	1. TANet青少年網路內容防護計畫執行 2. 其他交辦事項	2515	第一順序：張小姐 第二順序：佘先生
高級技術師	賴先生	hanz523ATmail.nsysu.edu.tw	1. TANet青少年網路內容防護計畫執行 2. 其他交辦事項	2500	第一順序：陳先生 第二順序：張小姐

2. 網路中心基礎維運

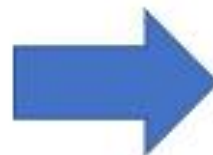
- 網路架構圖
- 網路流量管理
 - Cacti網管系統及Weathermap plugin
 - IPv4/IPv6流量現況
- 連線單位實地到訪
- 連線單位網路支援
- 精進網路管理
- 教育部DNS主機維運及主控台異地備援

高屏澎區網中心網路架構圖



Cacti網管系統及Weathermap plugin

- **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



Cacti網管系統及Weathermap plugin

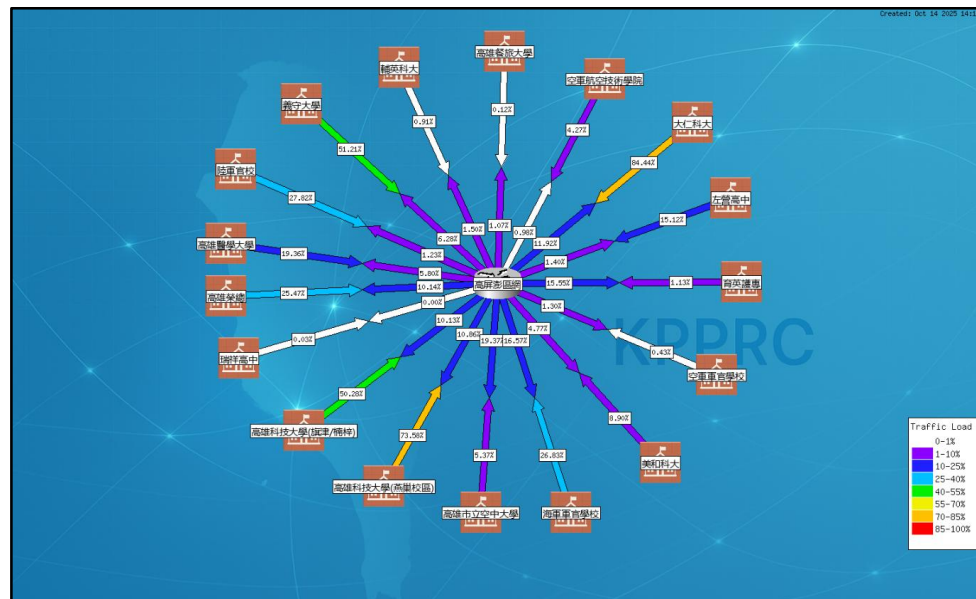
- **Cacti重新建置**：舊實體主機的Cacti監控軟體停機，改為虛擬主機並建置新的Cacti監控軟體



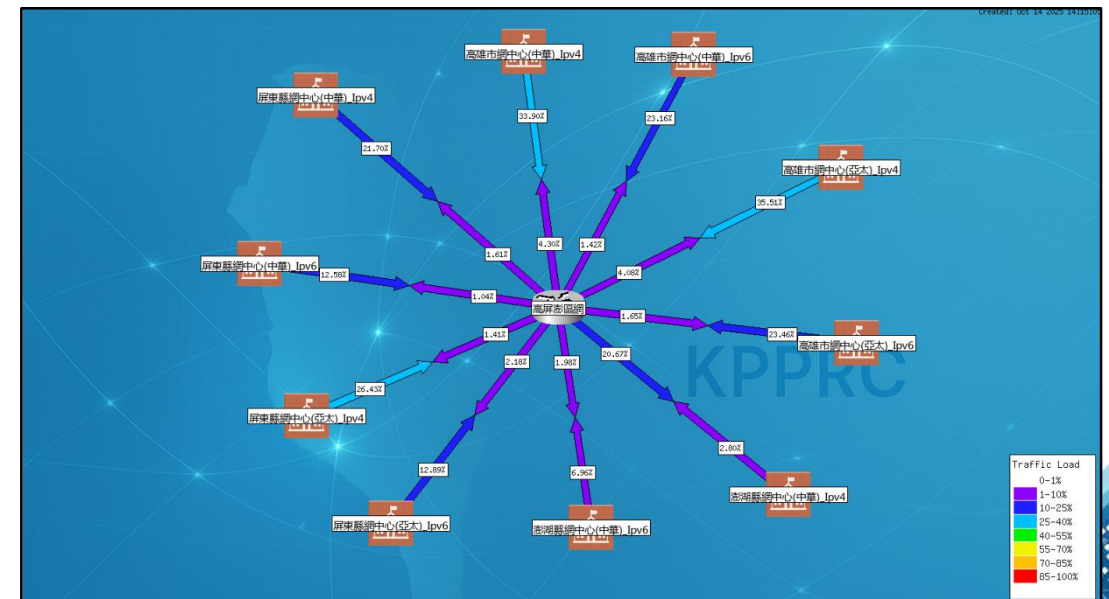
Cacti網管系統及Weathermap plugin

- 建置Weather Map：建置新的Weather Map：

下轄連線單位

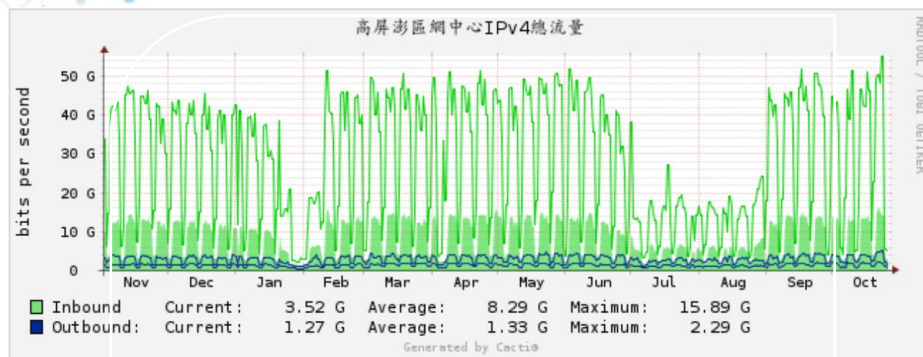


縣網連線單位



IPv4/IPv6流量現況

IPv4 Traffic



114年上半年

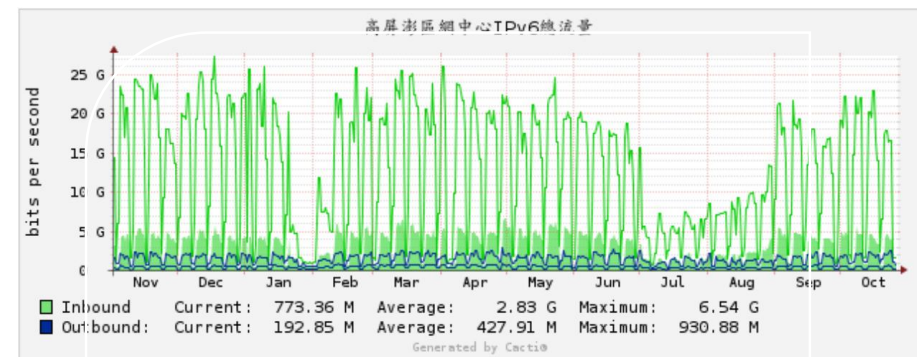
Maximum: 15.55G, Average: 7.85G

114年下半年

Maximum: 15.89G, Average: 8.29G



IPv6 Traffic



114年上半年

Maximum: 6.54G, Average: 2.70G

114年下半年

Maximum: 6.54G, Average: 2.83G



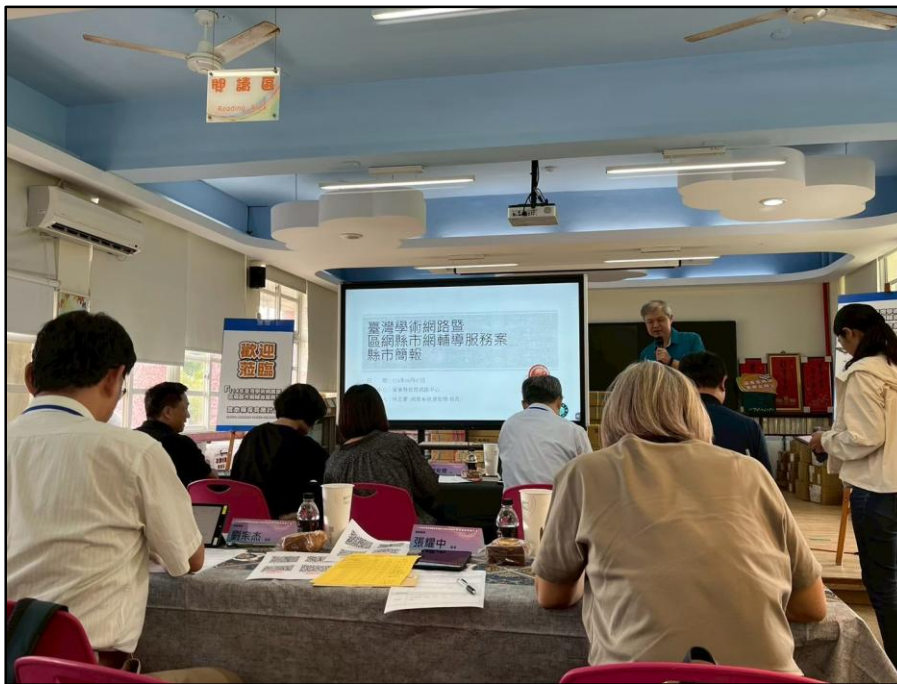
連線單位實地到訪(1/5)

- 協同教育部實地訪問高雄市網、屏東縣網及澎湖縣網
 - 高雄探訪：



連線單位實地到訪(1/5)

- 協同教育部實地訪問高雄市網、屏東縣網及澎湖縣網
 - 屏東探訪：



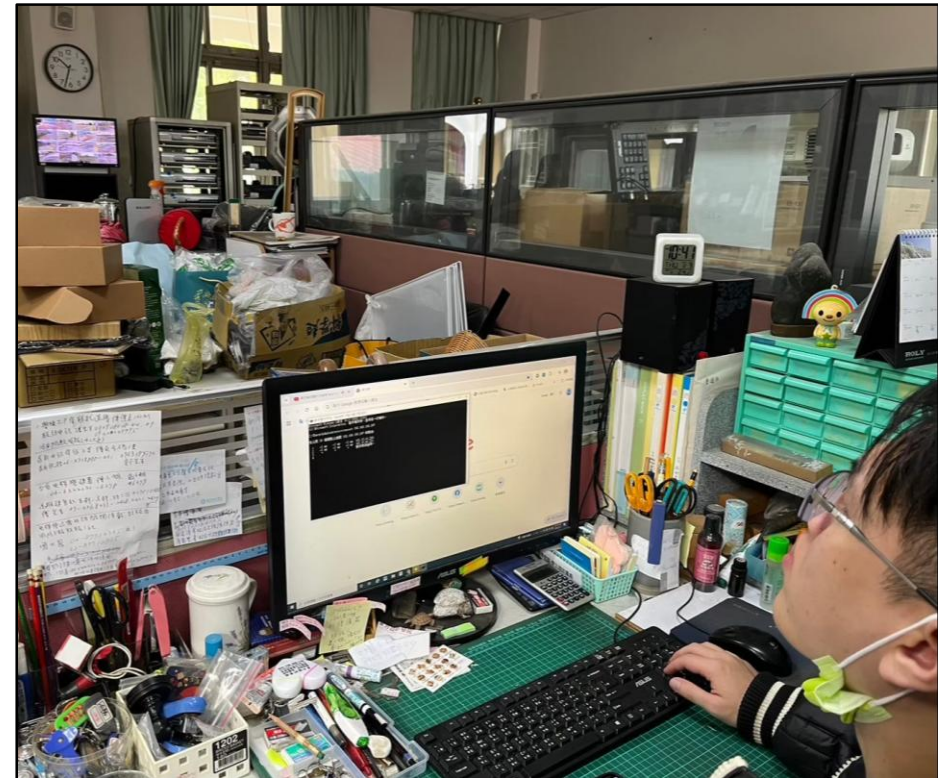
連線單位實地到訪(1/5)

- 協同教育部實地訪問了高雄市網、屏東縣網及澎湖縣網
 - 澎湖探訪：



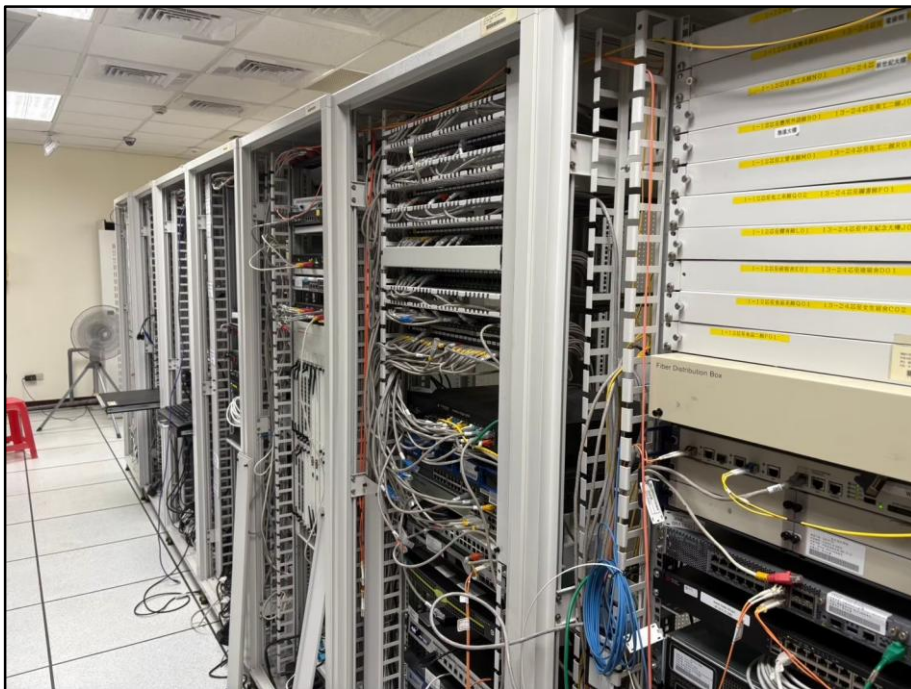
連線單位實地到訪(2/5)

- 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。



連線單位實地到訪(2/5)

- 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。



連線單位實地到訪(3/5)

- 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。



連線單位實地到訪(3/5)

- 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。



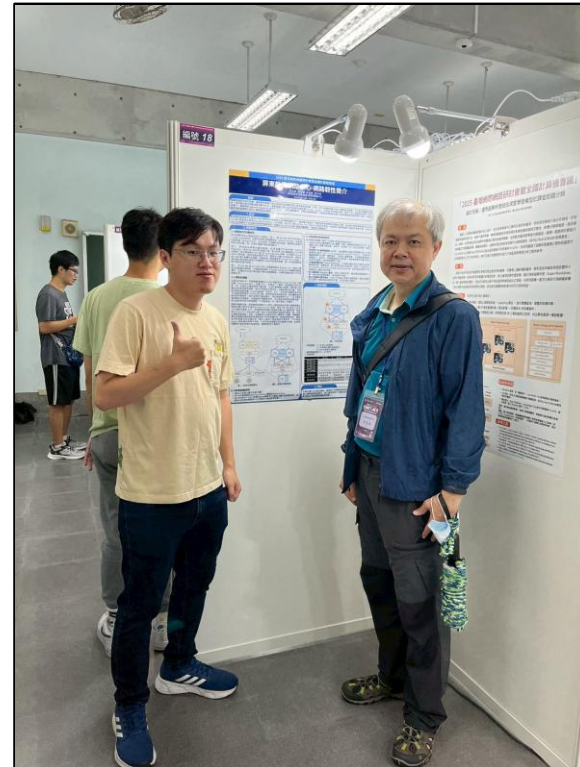
連線單位實地到訪(4/5)

- 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。



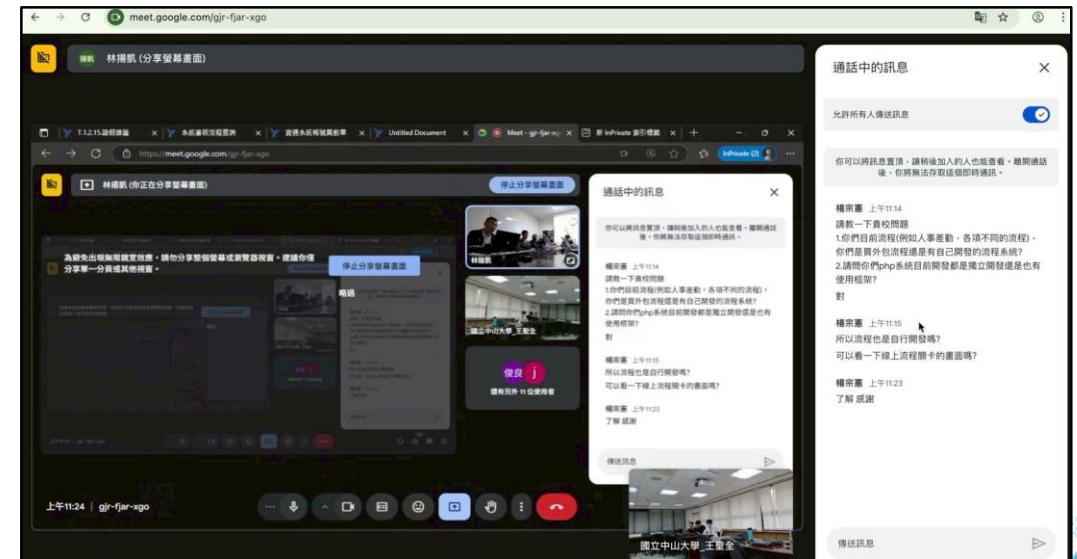
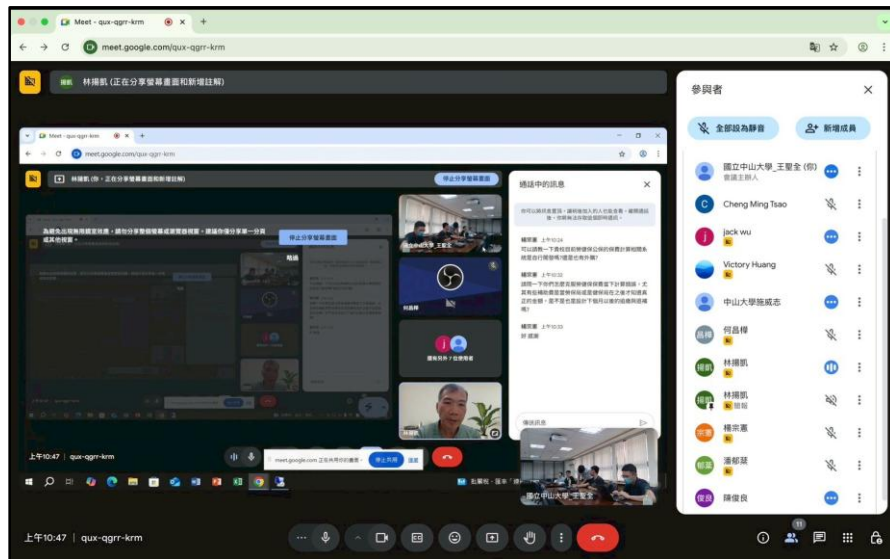
連線單位實地到訪(4/5)

- 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。



連線單位實地到訪(5/5)

- 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。



連線單位實地到訪(5/5)

- 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。



連線單位網路支援(1/6)

- **114年1月13日美和科技大學線路改接：**
 - 原中華電信 200M 線路調整為台灣大哥大 1G 連線。
- **處理結果：**
 - 已排定時程配合美和科大網管人員與台灣大哥大人員於114年1月13日完成線路更改，並啟用ipv6。

連線單位網路支援(2/6)

- **114年2月5日下轄學校反映受到DDOS攻擊：**
 - 下轄學校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。

連線單位網路支援(3/6)

- **114年4月11日區中斷和春技術學院連線服務：**
 - 因學校已關閉確認最後連線日期。
- **處理結果：**
 - 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。

連線單位網路支援(4/6)

- **114年5月17日澎湖縣網中心反映斷線：**
 - 澎湖縣網中心反映斷線，經查詢路由器及與中華電信確認，判斷為中華電信陸纜故障。
- **處理結果：**
 - 有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。
 - 建立PRTG監控，可供連線單位查看斷線及延遲。

連線單位網路支援(5/6)

- **114年7月14日下轄學校反映網路延遲：**
 - 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。

連線單位網路支援(6/6)

- **114年10月8日下轄學校反映不定時斷線及網路不穩：**
 - 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。
- **114年10月15日下轄學校反映不定時斷線及網路不穩：**
 - 10月15日上午9點00分詢問學校，因以前有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。

精進網路管理(1/4)

- 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。

名稱	修改日期	類型	大小
!資安單	2025/10/27 下午 04:13	檔案資料夾	
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	
1140113美和線路由中華電信改為台灣大...	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...	2025/3/4 下午 03:39	Microsoft Word ...	76 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(中殭屍病毒).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
1140912高科大第一校區iot掃描問題.do...	2025/10/14 上午 11:24	Microsoft Word ...	63 KB
1141013高雄餐旅大學網路都會陸陸續續...	2025/10/14 上午 11:29	Microsoft Word ...	128 KB
1141020育英醫專網路都會陸陸續續斷線...	2025/10/27 下午 03:56	Microsoft Word ...	234 KB

精進網路管理(2/4)

- 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。

!!測試指令	2025/1/21 下午 06:01	檔案
ccna1	2025/9/8 下午 08:13	檔案
DNS受攻擊	2024/5/21 上午 09:54	檔案
ipv6新增規則	2025/1/8 下午 01:27	檔案
ospf研究	2025/1/8 下午 01:25	檔案
SNMP搜尋	2024/6/11 下午 04:25	檔案
SQL 注入攻擊測試	2025/6/27 上午 08:29	檔案
TLS關閉教學	2024/7/3 下午 05:25	檔案
安裝https憑證	2025/6/27 上午 08:30	檔案
網頁部屬教學	2025/3/14 下午 04:38	檔案
遠傳指令	2024/5/21 上午 10:12	檔案
cmd指令.docx	2024/9/11 上午 09:11	Micro
RPZ DNS Server說明(內含dns設定說明)....	2025/4/24 下午 02:47	Micro
Shodan教學.docx	2025/9/12 上午 11:22	Micro
ubuntu指令.docx	2024/1/15 下午 03:06	Micro
區網dns添加網域教學.docx	2024/5/30 下午 01:58	Micro
專案Git設定及Gitlab推送方法.docx	2025/4/25 下午 05:02	Micro
網路.docx	2025/7/9 下午 03:00	Micro
網路0627.docx	2025/6/27 上午 08:27	Micro
瀏覽器指令.docx	2024/12/4 下午 12:06	Micro

精進網路管理(3/4)

• 盤點下轄學校網路資訊:

- 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

4	空軍航空技術學院	1G
5	大仁科大	500M
6	左營高中	300M
7	育英醫護管理專科學校	500M
8	空軍軍官學校	1G
9	美和科大	1G
10	海軍軍官學校	400M
11	高雄市立空中大學	1G
12	高雄科技大學(燕巢校區)	1G
13	高雄海洋科技大學	1G
14	高餐	1G
15	國立高雄大學	600M
16	國立高雄第一科技大學	1G
17	慈惠醫專	500M
18	瑞祥高中	1G
19	樹人醫護管理專科學校	400M
20	文藻大學	2G
21	和春技術學院	倒了
22	東方設計學院	倒了
23	台鋼科技大學	1G
24	高雄榮總(2019/2/22)	1G
25	高雄醫學大學	1G
26	國立屏東大學	1G
27	國立屏東科技大學	1G
28	國立高雄師範大學	1G
29	國立高雄師範大學(燕巢校區)	1G
30	國立高雄應用科技大學	1G
31	陸軍官校	1G
32	義守大學	1G
33	實踐大學-高雄校區	1G
34	輔英科大	1G
35	樹德科大	1G
36	中正預校	1G

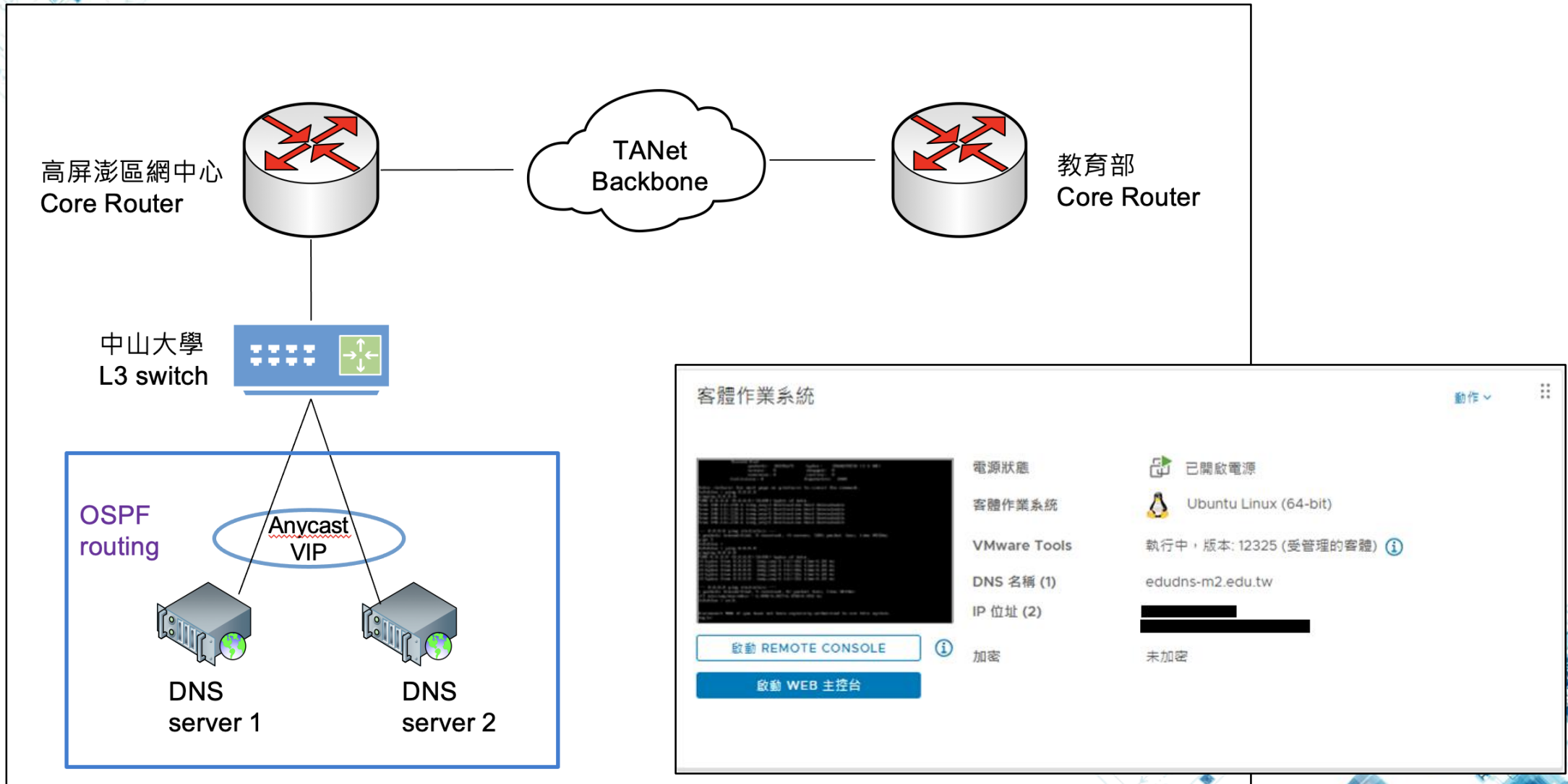
精進網路管理(4/4)

- 參加課程考取專業證照：CEH、CCNA1。



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

教育部DNS主機維運



3. 網路及資安技術支援

- 教育訓練辦理情形
- 資安通報事件處理時效
- 資安技術支援

教育訓練辦理情形

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

教育訓練辦理情形

- **區網管審會及教育訓練內容調整：**

- 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
- 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。
- 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。

資安通報事件處理時效

- 資安事件緊急通報處理之效率及通報率

113年

114年

所屬之學校及單位1、2級資安事件處理			
	通報平均時間	0.09小時	0.13小時
	應變處理平均時數	0.59小時	0.07小時
	事件處理平均時數	5.16小時	1小時
	通報完成率	100%	100%
	事件完成率	100%	100%
所屬之學校及單位3、4級資安事件通報：無任何3、4級事件			
	資安事件通報審核平均時數	2.91小時	6.03小時

資安通報事件處理時效

• 資安事件通報審核平均時數6小時：

- 原因：資安單發生時間為2025-04-12（六）19:28:39左右，因下班後無收到簡訊通知，故2025-04-14(一)上班才知道，後續有通知tacert做調整，後續正常收到簡訊通知。

詳細資料			
發佈編號	ASOC-105-202504-00000105	發佈時間	2025-04-12 19:00:20
事件類型	系統被入侵	發現時間	2025-04-12 10:50:01
事件主旨	[國立屏東科技大學]140.127.19.33 backdoor: Malware.Sinkhole		
事件描述	ASOC發現貴單位(國立屏東科技大學)所屬 140.127.19.33 疑似對外進行 backdoor: Malware.Sinkhole 攻擊		
手法研判			
處理建議	惠請貴單位：1.檢查防火牆紀錄：查看內部是否有開啟異常的連接埠。2.利用工具程式(如:TCPview、procexp)於來源主機觀察，找出實際執行連線的程式，確認該程式是否為惡意程式。3.若連線並非預期行為，則來源主機可能已遭植入惡意程式，建議利用木馬或後門清除程式掃描該主機，並主動檢測是否有惡意程式執行。4.確實部署防火牆並定期更新設備密碼。5.攻擊名稱相關參考資料網站：Fortinet-- https://fortiguard.com/encyclopedia/ips/46581 Other-- https://en.wikipedia.org/wiki/DNS_sinkhole		
參考資料			

1. 通報型態：	告知通報
告知通報編號：	ASOC-105-202504-00000105
2. 事件發生時間：	2025-04-12 10:50:01
3. 確認(知悉)為資安事件時間：	2025-04-12 19:53:44
4. 設備資料：	
I P 位置：	140.127.19.33
國際網路位置：	
設備廠牌、機型：	

改善時間：	2025-04-15 19:54:44
◎區縣市網通報審核	
通報審核結果:通過	
區縣市網審核時間:2025-04-14 08:27:00	
◎區縣市網應變審核	
區縣市網應變審核結果:通過	
區縣市網應變審核時間:2025-04-14 08:27:00	

資安通報事件處理時效

• 資安事件通報審核平均時數6小時：

- 原因：資安單發生時間為2025-04-12（六）19:28:39左右，因下班後無收到簡訊通知，故2025-04-14(一)上班才知道，後續有通知tacert做調整，後續正常收到簡訊通知。

詳細資料			
發佈編號	ASOC-105-202504-00000106	發佈時間	2025-04-12 19:00:21
事件類型	系統被入侵	發現時間	2025-04-12 10:50:03
事件主旨	[國立屏東科技大學]140.127.29.41 backdoor: Malware.Sinkhole		
事件描述	ASOC發現貴單位(國立屏東科技大學)所屬 140.127.29.41 疑似對外進行 backdoor: Malware.Sinkhole 攻擊		
手法研判			
處理建議	惠請貴單位： 1.檢查防火牆紀錄：查看內部是否有開啟異常的連接埠。 2.利用工具程式(如:TCPview、procexp)於來源主機觀察，找出實際執行連線的程式，確認該程式是否為惡意程式。 3.若連線並非預期行為，則來源主機可能已遭植入惡意程式，建議利用木馬或後門清除程式掃描該主機，並手動檢測是否有惡意程式執行。 4.確實部署防火牆並定期更新設備密碼。 5.攻擊名稱相關參考資料網站：Fortinet-- https://fortiguard.com/encyclopedia/ips/46581 Other-- https://en.wikipedia.org/wiki/DNS_sinkhole		
參考資料			

1. 通報型態：	告知通報
告知通報編號：	ASOC-105-202504-00000106
2. 事件發生時間：	2025-04-12 10:50:03
3. 確認(知悉)為資安事件時間：	2025-04-12 19:59:14
4. 設備資料：	
I P 位置：	140.127.29.41
網際網路位置：	
設備廠牌、機型：	

改善時間：	2025-04-15 19:54:44
◎區縣市網通報審核	
通報審核結果:通過	
區縣市網審核時間:2025-04-14 08:27:00	
◎區縣市網應變審核	
區縣市網應變審核結果:通過	
區縣市網應變審核時間:2025-04-14 08:27:00	

資安通報事件處理時效

• 資安事件通報審核平均時數6小時：

- 原因：資安單發生時間為2025-04-12（六）19:28:39左右，因下班後無收到簡訊通知，故2025-04-14(一)上班才知道，後續有通知tacert做調整，後續正常收到簡訊通知。

詳細資料			
發佈編號	ASOC-105-202504-00000116	發佈時間	2025-04-12 19:15:17
事件類型	對外攻擊	發現時間	2025-04-12 10:50:17
事件主旨	[國立高雄師範大學]140.127.42.68 backdoor: Malware.Sinkhole		
事件描述	ASOC發現貴單位(國立高雄師範大學)所屬 140.127.42.68 疑似對外進行 backdoor: Malware.Sinkhole 攻擊		
手法研判			
處理建議	惠請貴單位： 1.檢查防火牆紀錄：查看內部是否有開啟異常的連接埠。 2.利用工具程式(如:TCPview、procexp)於來源主機觀察，找出實際執行連線的程式，確認該程式是否為惡意程式。 3.若連線並非預期行為，則來源主機可能已遭植入惡意程式，建議利用木馬或後門清除程式掃描該主機，並手動檢測是否有惡意程式執行。 4.確實部署防火牆並定期更新設備密碼。 5.攻擊名稱相關參考資料網站：Fortinet-- https://fortiguard.com/encyclopedia/ips/46581 Other-- https://en.wikipedia.org/wiki/DNS_sinkhole		
參考資料			

1. 通報型態：	告知通報
告知通報編號：	ASOC-105-202504-00000116
2. 事件發生時間：	2025-04-12 10:50:17
3. 確認(知悉)為資安事件時間：	2025-04-12 19:28:39
4. 設備資料：	
I P 位置：	140.127.42.68
網際網路位置：	
設備廠牌、機型：	

改善時間：	2025-04-15 19:29:39
◎區縣市網通報審核	
通報審核結果:通過	
區縣市網審核時間:2025-04-14 08:26:21	
◎區縣市網應變審核	
區縣市網應變審核結果:通過	
區縣市網應變審核時間:2025-04-14 08:26:21	

資安通報事件處理時效

• 資安事件通報審核平均時數6小時：

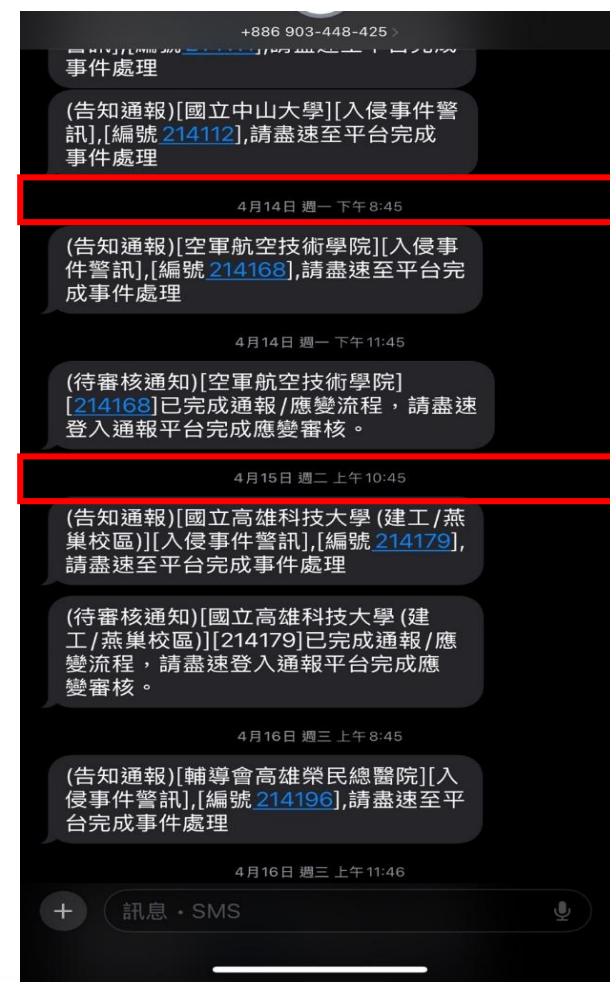
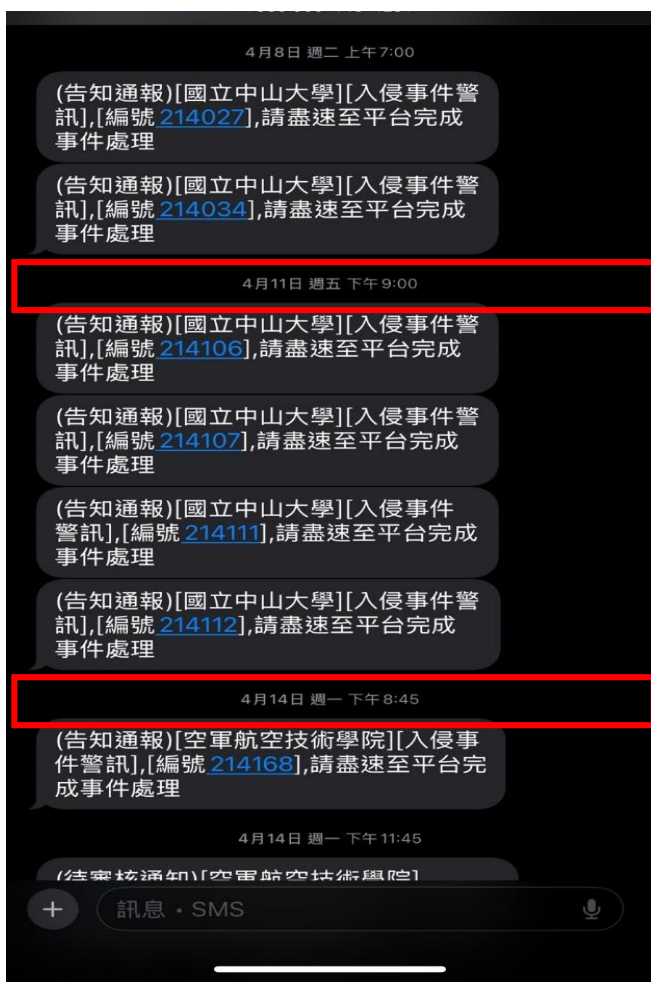
- 原因：資安單發生時間為2025-04-12（六）19:28:39左右，因下班後無收到簡訊通知，故2025-04-14(一)上班才知道，後續有通知tacert做調整，後續應該會正常收到。

通報單位	主旨	等級	事件類型	子類型	知悉時間	發佈時間	通報時間	應變時間	通報審核時間	ip	通報審核時間
國立中山大學		2級	INT	系統被入侵	2025-09-10 13:47:06	2025-09-10 13:50:30	2025-09-10 13:50:30	2025-09-10 13:50:30	2025-09-10 13:50:56	140.117.12.100	0:03:50
私立高雄醫學大學	A-ISAC高雄醫學大學之內容管理系統(CMS)內容疑似遭駭客入侵	1級	INT	系統被入侵	2025-08-05 15:33:00	2025-08-05 15:30:13	2025-08-05 15:59:46	2025-08-05 15:59:46	2025-08-05 16:01:12	163.15.154.43	0:28:12
高雄市立空中大學		2級	FAC	拒絕服務(DDOS)	2025-06-07 08:40:33	2025-06-07 08:52:20	2025-06-07 08:52:20	2025-06-07 10:13:49	2025-06-07 09:33:43	163.15.183.91	0:53:10
國立高雄師範大學	國立高雄師範大學[140.127.42.68] backdoor: Malware, Sinkhole	1級	INT	對外攻擊	2025-04-12 19:28:39	2025-04-12 19:15:17	2025-04-12 19:36:58	2025-04-12 19:36:58	2025-04-14 08:26:21	140.127.42.68	36:57:42
國立屏東科技大學	國立屏東科技大學[140.127.29.41] backdoor: Malware, Sinkhole	1級	INT	系統被入侵	2025-04-12 19:59:14	2025-04-12 19:00:21	2025-04-12 20:01:47	2025-04-12 20:01:47	2025-04-14 08:26:52	140.127.29.41	36:27:38
國立屏東科技大學	國立屏東科技大學[140.127.19.33] backdoor: Malware, Sinkhole	1級	INT	系統被入侵	2025-04-12 19:53:44	2025-04-12 19:00:20	2025-04-12 20:00:08	2025-04-12 20:00:08	2025-04-14 08:27:00	140.127.19.33	36:33:16
正修科技大學	[正修科技大學]120.118.146.111 backdoor: Malware, Sinkhole	1級	INT	系統被入侵	2025-04-08 08:24:00	2025-04-08 07:00:41	2025-04-08 08:29:43	2025-04-08 08:29:43	2025-04-08 08:31:31	120.118.146.111	0:07:31
私立樹德科技大學	教育部資安通告-私立樹德科技大學[120.119.126.66]主機遭入侵	1級	INT	系統被入侵	2025-03-18 09:06:25	2025-03-18 09:00:14	2025-03-18 09:12:04	2025-03-18 09:12:04	2025-03-18 09:21:03	120.119.126.66	0:14:38
國立高雄大學	教育部資安通告-國立高雄大學[140.127.224.0]OpenSSH 競爭	1級	INT	系統被入侵	2025-03-06 14:54:33	2025-03-06 14:45:22	2025-03-06 15:03:06	2025-03-06 15:03:06	2025-03-06 15:17:42	140.127.224.0	0:23:09
私立高雄醫學大學		1級	DEF	惡意網頁	2025-03-05 17:18:39	2025-03-05 17:20:39	2025-03-05 17:20:39	2025-03-05 17:20:39	2025-03-05 17:32:13	163.15.172.112	0:13:34
國立屏東科技大學	國立屏東科技大學[140.127.15.154:8080] 存在弱密碼(Weak Passwords)	1級	INT	系統被入侵	2025-02-25 10:31:10	2025-02-25 10:30:19	2025-02-25 10:48:31	2025-02-25 10:48:31	2025-02-25 10:50:56	140.127.15.154	0:19:46
國立屏東科技大學	國立屏東科技大學[140.127.2.151:8080] 存在弱密碼(Weak Passwords)	1級	INT	系統被入侵	2025-02-25 10:47:36	2025-02-25 10:30:18	2025-02-25 10:50:51	2025-02-25 10:50:51	2025-02-25 10:51:15	140.127.2.151	0:03:39
私立高雄醫學大學	高雄醫學大學醫研大樓實驗動物中心[163.15.177.19] 存在弱密碼(Weak Passwords)	1級	INT	系統被入侵	2025-02-25 10:37:44	2025-02-25 10:30:14	2025-02-25 10:44:03	2025-02-25 10:44:03	2025-02-25 10:46:39	163.15.177.19	0:08:55
私立高雄醫學大學	高雄醫學大學[163.15.157.61] 存在弱密碼(Weak Passwords)	1級	INT	系統被入侵	2025-02-25 10:25:24	2025-02-25 10:15:22	2025-02-25 10:38:32	2025-02-25 10:38:32	2025-02-25 10:46:50	163.15.157.61	0:21:26
國立高雄大學	貴單位遭受外部DDOS攻擊	1級	FAC	拒絕服務(DDOS)	2025-02-05 18:56:11	2025-02-05 18:59:24	2025-02-05 18:59:24	2025-02-05 18:59:24	2025-02-05 20:21:58	140.127.198.2	1:25:47
國立高雄大學	貴單位遭受外部DDOS攻擊	1級	FAC	拒絕服務(DDOS)	2025-02-05 18:47:30	2025-02-05 18:57:07	2025-02-05 18:57:07	2025-02-05 18:57:07	2025-02-05 20:22:09	140.127.198.1	1:34:39
輔導會高雄榮民總醫院	[輔導會高雄榮民總醫院]203.68.96.125 applications3: MS, ISA, IIS	1級	INT	系統被入侵	2025-01-24 09:52:27	2025-01-23 23:00:13	2025-01-24 09:55:36	2025-01-24 09:55:36	2025-01-24 10:10:32	203.68.96.125	0:18:05
國立高雄師範大學	A-ISAC 國立高雄師範大學網站發現資訊洩漏	1級	DEF	惡意網頁	2025-01-15 16:18:17	2025-01-15 16:15:13	2025-01-15 16:23:46	2025-01-15 16:23:46	2025-01-15 16:31:41	140.127.50.30	0:13:24
私立義守大學	教育部資安通告-私立義守大學[140.127.181.243]Moxa 設備遭入侵	1級	INT	系統被入侵	2025-01-08 14:08:24	2025-01-08 13:45:21	2025-01-08 14:09:45	2025-01-08 14:09:45	2025-01-08 14:20:26	140.127.181.24	0:12:02
										平均總計	6:09:30

資安通報事件處理時效

• 資安事件通報審核平均時數6小時：

- 原因：資安單發生時間為2025-04-12（六）19:28:39左右，因下班後無收到簡訊通知，故2025-04-14(一)上班才知道，後續有通知tacert做調整，後續有正常收到簡訊。



資安通報事件處理時效

- 資安事件通報審核平均時數6小時：

- 改善方式：與Tacert討論，如資安事件單有問題，需送單前向Tacert反應，事後反應無法做任何調整。

縣市區網單位使用EVS線上平台進行弱點掃描

- 每年通知各連線單位，進行系統弱點進行修補，並於成大弱掃平台進行複測。
- 提供各連線單位，如有任何問題可隨時來電協助系統弱點修補協助。



成大弱點掃描服務使用注意事項

- 1.申請弱掃網站需有SSL憑證。
- 2.非區網中心可同時排程數量5個。
- 3.周末、例假日不提供排程。
- 4.避免同時段掃描該單位多網站。
- 5.掃描前請進行備份、設定白名單、整理網站目錄、避開公務時間掃描，或提前公告。
- 6.掃描超過7小時系統自動中斷，報告仍有效，請修正完後繼續複掃。
- 7.掃描低於1分鐘皆不會產生報告，請檢察防火牆開通狀態，或目標伺服器是否正常。
- 8.務必對中高風險優先修補。
- 9.單位已停用網站曾在EVS上掃描，請於平台上註記已停用。
- 10.已送出排程無法取消，需2天前電話通知成大團隊取消。
- 11.已弱掃的網站，需進行修補與追蹤。

 KPPRC高屏澎區網中心

縣市區網單位使用EVS線上平台進行弱點掃描

- 每年通知各連線單位，進行系統弱點進行修補，並於成大弱掃平台進行複測。

單位	網站	最新檢測		狀態	風險						
		網站網址 網站名稱 建立時間 重要程度	排程日期 ▼		嚴重風險	高風險	中風險	低風險	信息		
國立高雄師範大學	(新2021) 公文系統 2021-05-06 13:46 普通		2025-10-07 09:00	執行完成	0	0	1	1	4	修改	檢測記錄
大仁科技大學	 Web94 2022-01-17 09:34 普通		2025-10-07 00:00	執行完成	0	0	0	2	4	修改	檢測記錄
大仁科技大學	 選課95 2021-05-05 14:45 高		2025-10-07 00:00	執行完成	0	0	0	2	4	修改	檢測記錄
國立屏東大學	 圖書館網頁-2020 2020-06-15 11:52 普通		2025-09-26 00:00	執行完成	0	0	0	8	5	修改	檢測記錄
大仁科技大學	館藏查詢 2018-12-12 09:21 普通		2025-09-23 00:00	執行失敗	0	3	9	88	9	修改	檢測記錄
國立屏東大學	測驗與評量實驗室 2025-09-16 10:19 低		2025-09-22 17:00	執行完成	0	1	17	11	20	修改	檢測記錄
義守大學	系所暨教師表現系統 2024-09-20 10:57 普通		2025-09-19 17:00	執行失敗	0	7	11	12	8	修改	檢測記錄
義守大學	社團管理系統 2024-09-20 10:56 普通		2025-09-19 17:00	執行完成	0	1	5	6	5	修改	檢測記錄
義守大學	中程校務發展系統 2024-07-08 16:03		2025-09-19 00:00	執行完成	11	4	3	2	2	修改	檢測記錄

高屏澎區網中心-資安技術支援

- 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非上班時間，又有一小時需通報完成問題，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。

高屏澎區網中心-資安技術支援

- 下轄學校IoT通報多筆:
 - 原因：發現下轄學校有多筆IoT資安單通報，去電詢問狀況，得知未有有效掃描IoT清單的方式。
 - 處理：提供本校掃描IoT的教學檔供下轄學校參考。

詳細資料	詳細資料	詳細資料	詳細資料	詳細資料	詳細資料
發佈編號	發佈編號	NTUSOC-107-202509-ntuasoc-20250911-105502	發佈時間	2025-09-12 09:45:20	
事件類型	事件類型	威脅情報	發現時間	2025-09-12 09:13:23	
事件主旨	事件主旨	教育部資安通告-國立高雄第一科技大學[]印表機管理介面暴露在公開網路(NASOC-Rule INDICATOR-SCAN Printer management interface exposed to public network)			
事件描述	事件描述	北區ASOC發現IP: []的印表機管理介面暴露在公開網路上，可能導致未授權存取、漏洞利用、資料洩漏、遭受DoS攻擊等等。			
手法研判	手法研判	處理建議	1.若需要外部存取，建議限制存取範圍。 2.將管理介面移至內網。 3.若管理介面支援帳號管控功能，建議啟用以強化存取控制。		
處理建議	處理建議	參考資料			
參考資料	參考資料				

高屏澎區網中心-資安技術支援

- **轉發ANA預警通知信與IoT暴露名單:**
 - 將 ANA 事件單通知信共282封轉發給各下轄資安人員，如有問題可再提供協助。
 - 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。

4. 特色服務

- 黑名單系統 (區網下轄各單位情資共享)
- PRTG監控系統



黑名單系統

黑名單系統-區網下轄各單位情資共享

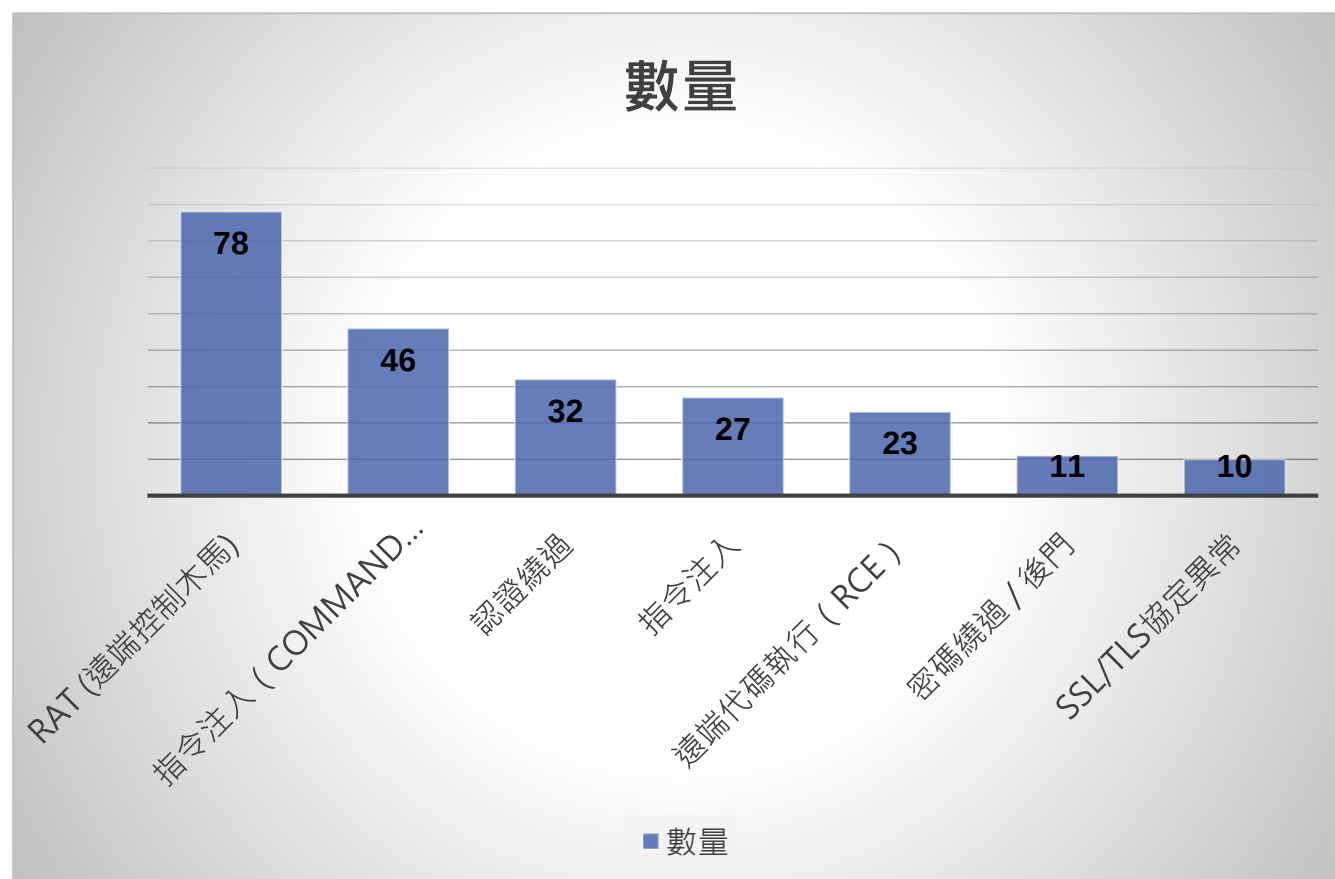
- 網址：<https://blacklist.kpprc.edu.tw/login>



The screenshot shows a web browser window with the title "登入 - 高屏澎區網黑名單系統". The address bar displays "blacklist.kpprc.edu.tw/login". The page content includes the title "黑名單系統" and a message: "若沒有帳號密碼，請向高屏澎區網中心申請". Below this, there are two input fields: "帳號" (Username) with the placeholder "請輸入帳號" and "密碼" (Password) with the placeholder "請輸入密碼". At the bottom, there is a green timestamp "最後更新時間：2025-10-24 08:10:02" and a blue "登入" (Login) button. A small "隱私權 - 條款" (Privacy Policy - Terms) link is visible in the bottom right corner.

黑名單系統-區網下轄各單位情資共享

- 網址：<https://blacklist.kpprc.edu.tw/login>



黑名單系統-區網下轄各單位情資共享

- 網址：<https://blacklist.kpprc.edu.tw/login>

#	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 UDPServer 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

黑名單系統-資安提升

- 黑名單系統已於成大弱掃並修復漏洞
- 黑名單系統調整安全政策（CSP）。
- 限制國外IP存取

EVS

網站弱點檢測

資安弱掃課程

系統資訊

連絡資訊

Hello EVS049

登出

高屏澎黑名單系統

檢測記錄

排程日期	檢測狀態	弱掃狀態	嚴重風險	高風險	中風險	低風險	信 息	威脅等級	更新日期	檢測結果	弱掃報告
2025-05-12 17:00	執行完成	completed	0	0	0	0	8	安全	2025-05-12 17:13	瀏覽	報告下載
2024-09-09 17:00	執行完成	completed	0	0	1	0	8	中	2024-09-09 17:10	瀏覽	報告下載
2024-08-29 17:00	執行完成	completed	0	0	3	1	3	中	2024-08-29 17:12	瀏覽	報告下載

黑名單系統-上傳檔案

高屏澎區網黑名單系統

blacklist.kpprc.edu.tw/my-uploaded-files

我的上傳檔案

黑名單系統

可上傳黑名單檔案，進行審核

*IP (Excel 或 CSV 或 ODS 檔)

選擇檔案 未選擇...何檔案 送出

注意事項：
一定要是 Excel 或 CSV 或 ODS 檔喔!
一定要有 ip 和 reason 欄位喔!

檔案名稱 上傳檔案用戶端 IP 狀態 上傳檔案時間 執行

Filter by 檔案名稱 X Filter by 上傳檔案... X Filter by 狀態 X Filter by 上傳檔... X

	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

黑名單系統-黑名單下載

黑名單系統

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

批次刪除黑名單 IP

使用者管理

管理者設定

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
118.86.231.105	Zyxel.Firmware.error.message.Command.Injection

黑名單系統-惡意網域、IP

惡意網域黑名單

www.	518.softether.net
iot8	softether.net
offi	gq
clou	e.co
offi	machine.xyz
gmai	machine.xyz
yaho	machine.xyz
turi	xyz
offi	work.gd
supp	aspersky.top
cdn-	aspersky.top
engl	news.online
www.	n.xyz
mail	mireland.com
logi	mireland.com
webs	
ched	id.ignorelist.com
shar	com
getf	
elec	com
meet	com
ivib	
driv	om
logi	om
getf	om
itri	net
azue	
webm	fgh.com
gtas	

已限制僅下轄學校IP可使用

惡意IP黑名單

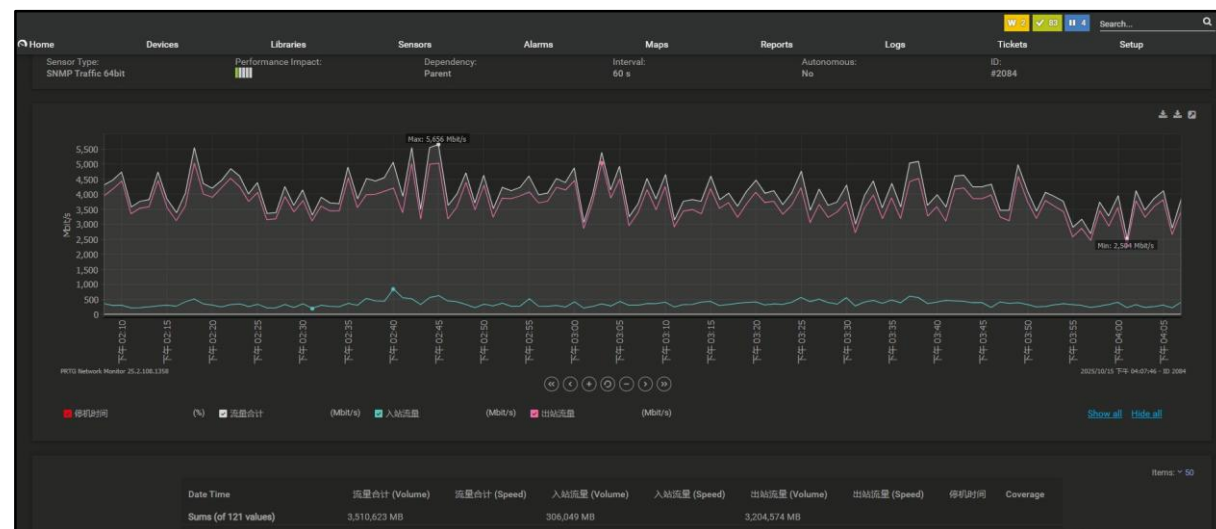
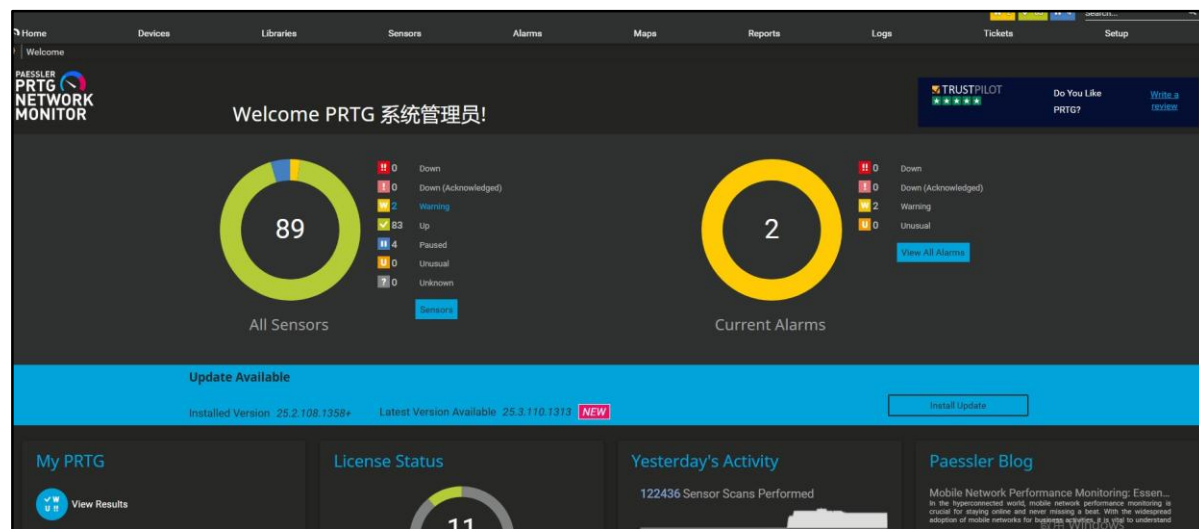
19	2
12	
19	6
69	
10	8
21	
60	
11	0
36	
14	
15	23
15	5
15	6
14	3
15	28
45	
16	
17	
93	
89	
80	2
10	3
16	72
21	0
21	8
10	5
11	7
13	
13	0
17	99
21	
17	4
17	27
14	
64	
67	
10	27
42	
10	6
14	
66	
66	
18	62
83	
18	5
45	
19	9
83	
67	2
18	



PRTG 監控系統

PRTG 監控系統(1/3)

- PRTG流量監控：提供詳細設備狀況、流量、延遲及掉包狀況。



PRTG 監控系統(1/3)

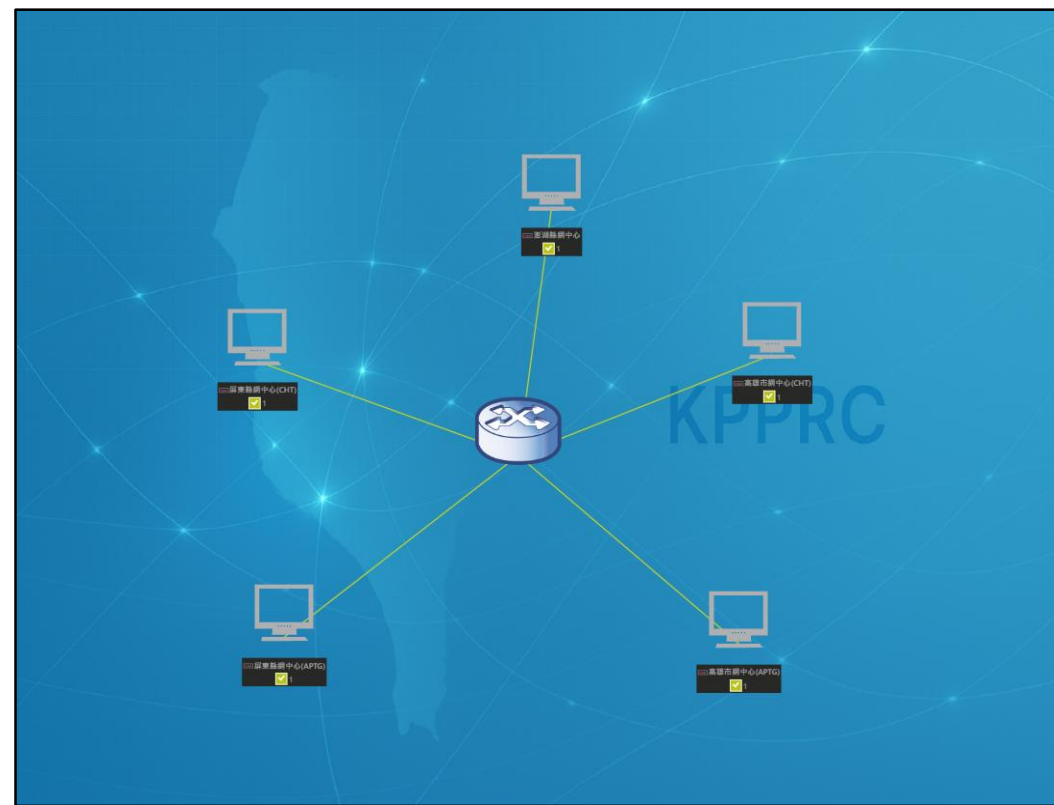
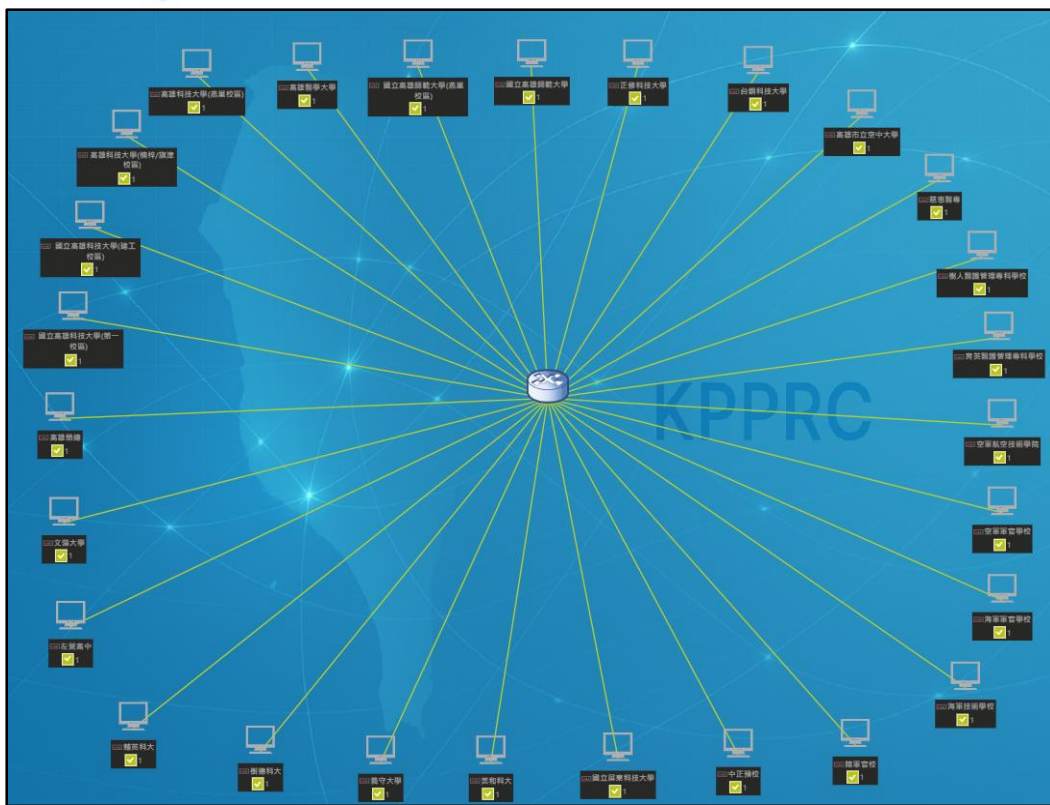
- PRTG流量監控：提供詳細設備狀況、流量、延遲及掉包狀況。

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 %

PRTG 監控系統(2/3)

- **PRTG流量監控**：提供下轄學校即時監控斷線網路圖。



PRTG 監控系統(3/3)

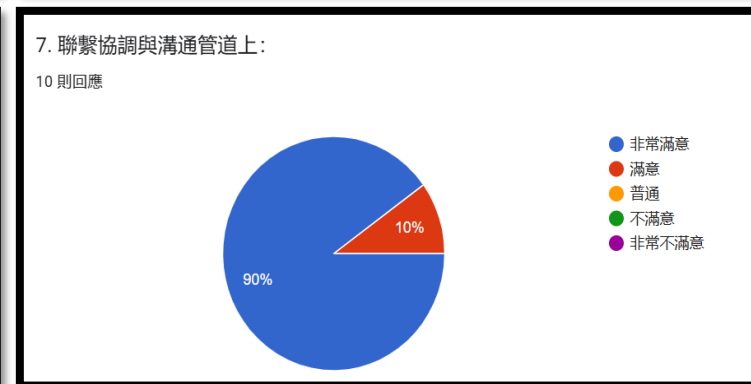
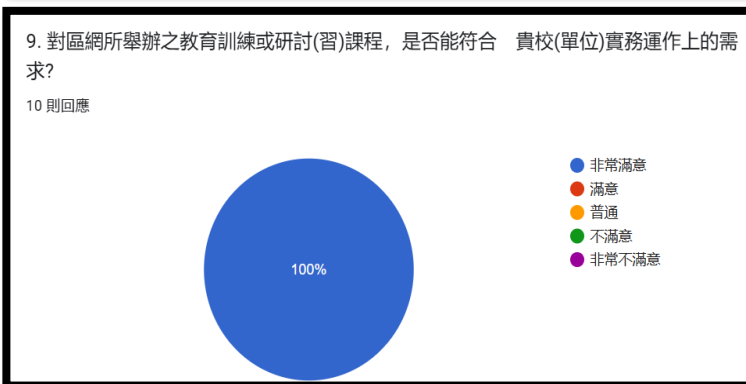
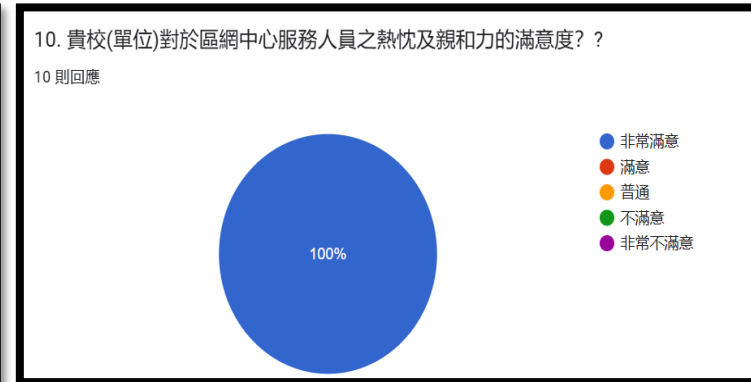
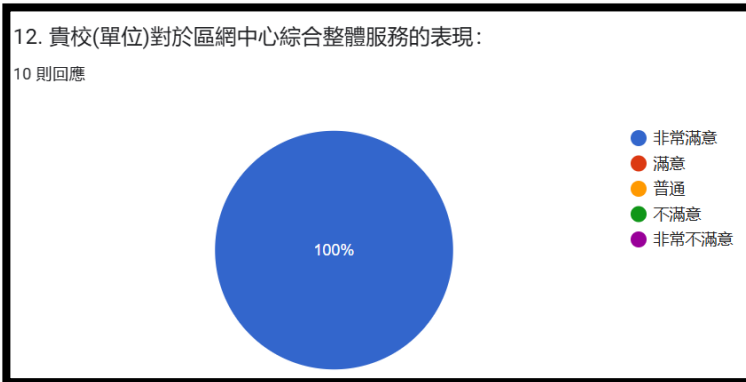
- PRTG流量監控：透過 PRTG 建立網路流量監控機制，設定延遲與中斷警示門檻，能在異常發生的第一時間即時通知管理人員，確保問題能迅速被發現與處理。

5. 連線單位需求分析及滿意度調查

- 區網服務滿意度問卷調查

服務滿意度問卷調查結果

➤ 今年服務人員熱忱及親和力滿意度總和達100%



6.未來營運目標

115年度預計推動之重點工作

- 資訊安全
 - 黑名單系統：持續優化黑名單系統，並納入更多元的黑名單。
 - 依據成大弱點掃描結果進行系統盤點與風險評估，協助下轄學校針對過舊或高風險系統加速修補與汰換。
- 網路管理
 - 推出各項監測服務系統如NETBOX、N-Reporter sflow，提供給需要的連線單位進行使用。
 - 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。
 - 盤點下轄學校中網路連線不穩定的單位，規劃分階段更換 GBIC 模組，並持續追蹤改善情形。
- 技術交流
 - 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。
 - 持續規劃並提供多元化的教育訓練課程與主題，強化下轄學校單位在資安防護與網路管理等面向的專業能力。
 - 加強人員教育訓練，提供更好的資訊技術及資安服務。



敬請 委員指教
謝謝!!

