



桃園區域網路中心 111年度執行成效 報告

單位：桃園區網中心

報告人：許時準 組長

Email：center20@ncu.edu.tw

電話：03-4227151#57507

日期：2022/11/17

2022



簡報大綱

1

經費與人力

2

網路管理

3

資安服務

4

特色服務、未來營運方針

5

成效精進、KPI

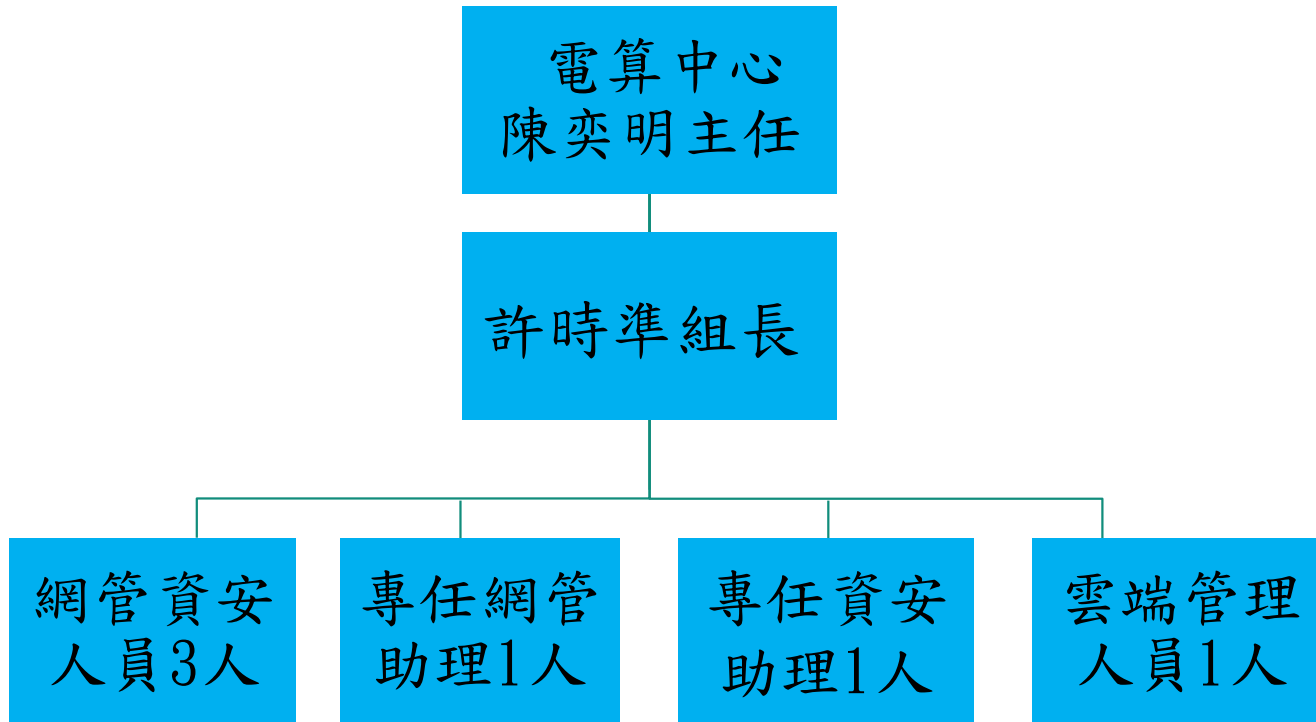


第一章



經費與人力





桃園區網經費統計

核定計畫金額	4,915,500
教育部補助金額	3,655,500
自籌金額	1,260,000
實際累計執行數 (至11月)	92.57%

108-110經費使用達成率

年度	計畫經費(核定數) 執行率	計畫補助金額 執行率
108年	98.91%	98.52%
109年	99.99%	99.99%
110年	100%	100%

- (一)本中心積極推動計畫規劃項目，同時本摶節原則及落實經費管控確實執行計畫補助經費，108~110年計畫核定經費、補助經費執行率均達98%以上。
- (二)108年度繳回人事費差額賸餘經費51,863元整，事因人事費經費編列時概估隔年度雇主負擔勞、健保調整額度，及進用專任助理學經歷(職級)之差異所造成之賸餘數。
- (三)自109年度起，計畫進用3名專任助理均依原編列職級聘用故已無人事費賸餘數。

專任網管人員任務與績效

網管人員(1位)的任務與績效

維護區網網路正常連線，線路異常排除

通訊網路設備管理

建置網路管理系統，DNS 及WWW server管理

機房及基礎環境(電力、空調、溫濕度、消防設備)
)維護

辦理網路管理技術研討會，臨時交辦事項。

專任資安人員任務與績效

資安人員(1位)的任務與績效

資安通報審核及演練，資安事件處理

異常流量IP偵測及處理

協助ISO27001資安認證，個資保護系統維護

弱點掃描，網頁檢測及追蹤處理

辦理資安研討會，臨時交辦事項。

雲端管理人員任務與績效

雲端管理人員(1位)的任務與績效

配合教育部資安政策，定期修改防火牆相關設定

協助臨時性防火牆調度支援教育部，以及備用機器歸還事宜

維護北區雲端資料中心儲存空間、網路設備、運算主機正常運作，並處理異常排除

建置北區雲端資料中心遠端連線設備權限設定並定期更新

協助連線單位處理雲端服務相關問題，臨時交辦事項



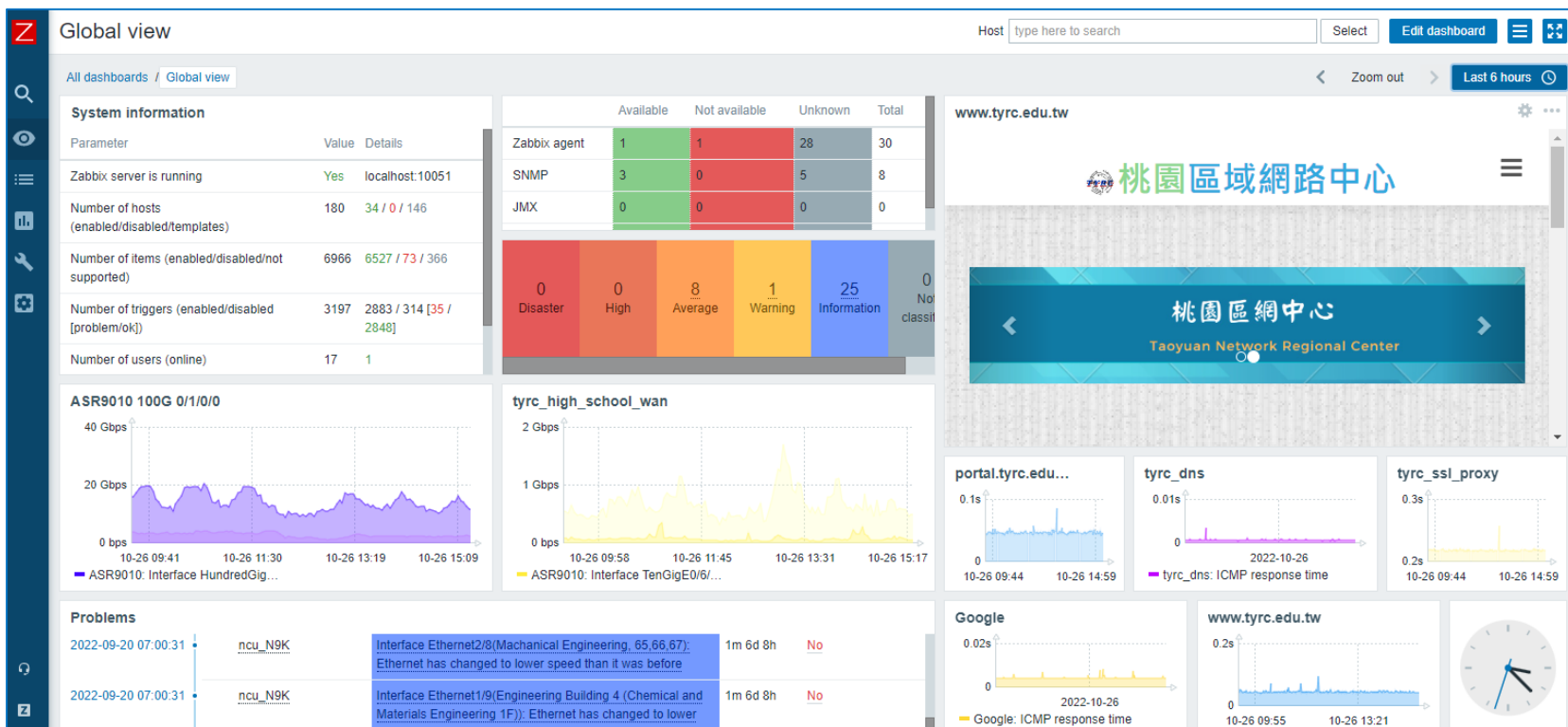
第一章



網路管理

自動監測系統結合自行開發LINE Notify

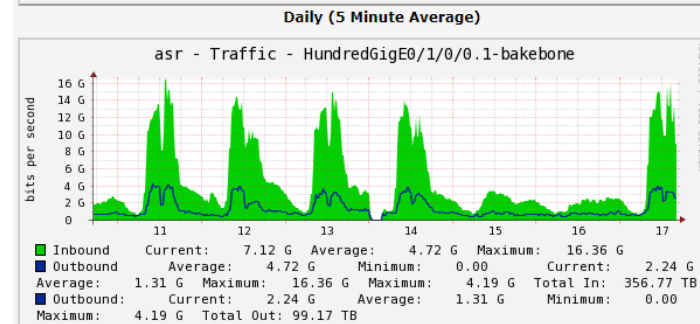
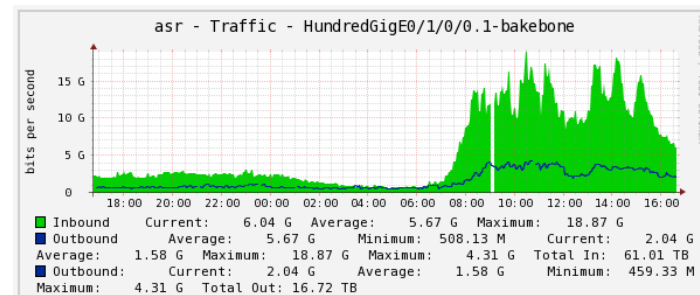
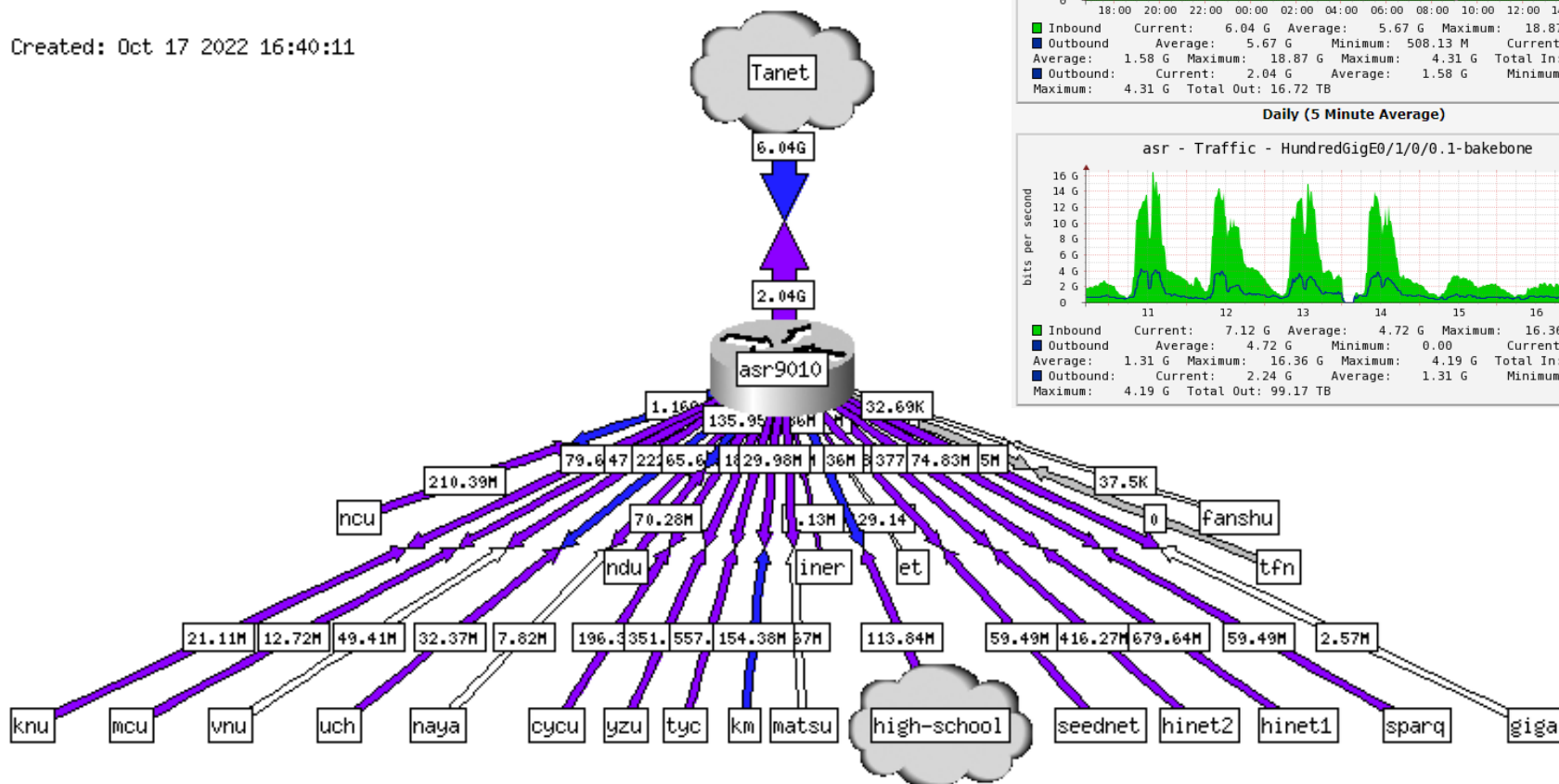
- ❑ 建置開源自動監測系統，針對重要網路設備、機房溫溼度監測、實體及虛擬伺服器的服務效能，利用自動化程序監測。
- ❑ 自行開發LINE Notify程式，進行LINE即時訊息自動發送警示訊息，及早發現問題並立即處理。



<https://zabbix.tyc.edu.tw/>

桃園區網Cacti系統監控流量

Created: Oct 17 2022 16:40:11



<https://cacti.tyrc.edu.tw/tyrc.html>

桃園區網高中職流量

桃園區域連線 網路使用統計圖

1. 桃園農工 [FE]	2. 至善工商 [FE]	3. 新興高中 [FE]	4. 育達高中 [FE]
5. 治平中學 [FE]	6. 六和高中 [FE]	7. 中壢高中 [FE]	8. 啟英高中 [FE]
9. 永平工商 [FE]	10. 大興工商 [FE]	11. 復旦中學 [FE]	12. 成功工商 [FE]
13. 清華高中 [FE]	14. 振聲高中 [FE]	15. 大華中學 [FE]	16. 中央警察大學 [FE]
17. Uplink [GE]			

寬頻上網 ⓘ

所有區域 所有類別 所有資源群組 所有狀態

總電路 17 請輸入搜尋關鍵字

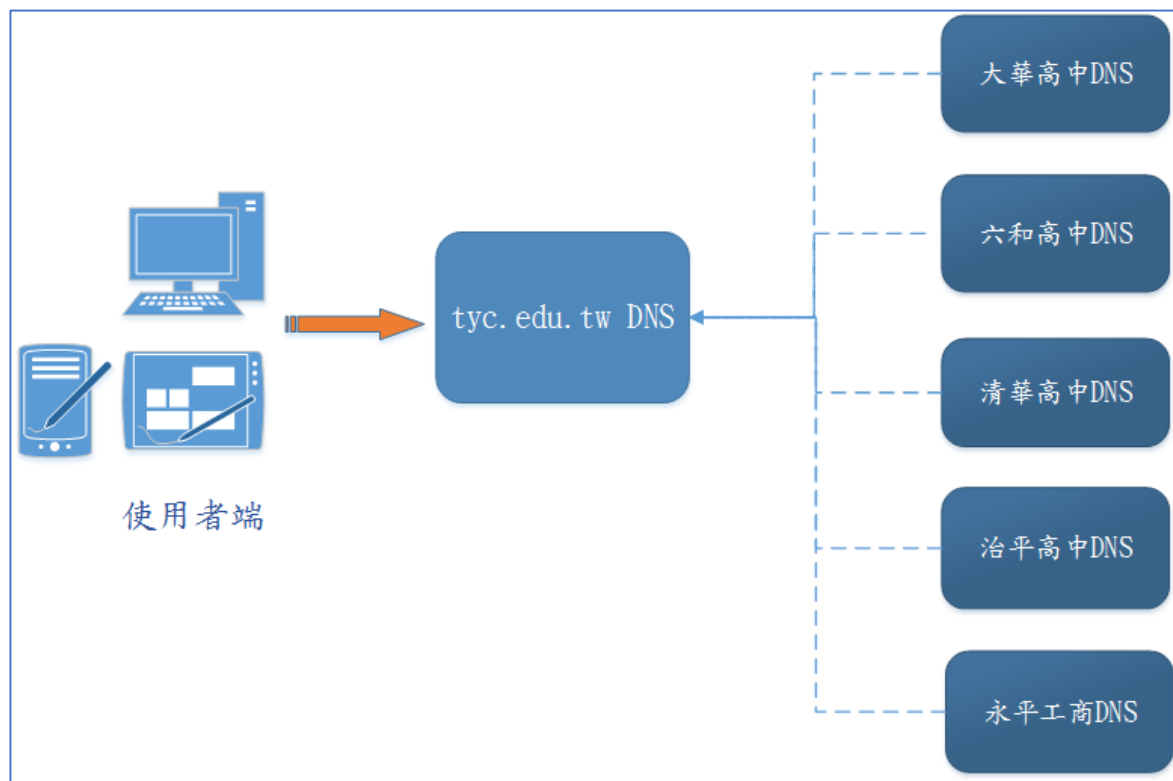
#	電路名稱/ 專線號碼 ▲	頻寬使用率	
		流入	流出
OTHERS		頻寬: 2500M	頻寬: 2500M
1	國立中央大學 (FTTS專線免出帳公報 電路) 34YV000163	流入: --- 流入頻寬使用率 0%	流出: --- 流出頻寬使用率 0%
2	FTTx 中央警察大學 33YV000367	頻寬: 300M 流入: 159777.97 Kbps 流入頻寬使用率 53.26%	頻寬: 300M 流出: 10343.11 Kbps 流出頻寬使用率 3.45%
3	FTTx 六和學校財團法人 桃園市六和高級中等學 校 34YV000169	頻寬: 300M 流入: 8495.96 Kbps 流入頻寬使用率 2.83%	頻寬: 300M 流出: 1923.21 Kbps 流出頻寬使用率 0.64%
4	FTTx 天主教輔聖學校財 團法人桃園市振聲高級 中等學校 33YV000360	頻寬: 300M 流入: 12365.39 Kbps 流入頻寬使用率 4.12%	頻寬: 300M 流出: 4810.34 Kbps 流出頻寬使用率 1.6%
5	FTTx 台灣省桃園縣私立 復旦高級中學 34YV000167	頻寬: 300M 流入: 6586.4 Kbps 流入頻寬使用率 2.2%	頻寬: 300M 流出: 2034.39 Kbps 流出頻寬使用率 0.68%
6	FTTx 永平學校財團法人 桃園市私立永平工商 高級中等學校 3478YV000030	頻寬: 300M 流入: 13066.43 Kbps 流入頻寬使用率 4.36%	頻寬: 300M 流出: 3938.2 Kbps 流出頻寬使用率 1.31%
7	FTTx 治平學校財團法人 桃園市治平高級中等學 校 3478YV000028	頻寬: 300M 流入: 33777.82 Kbps 流入頻寬使用率 11.26%	頻寬: 300M 流出: 5839.12 Kbps 流出頻寬使用率 1.95%



<https://cacti.tyrc.edu.tw/high-school.html>

高中職 DNS 向上集中(1)

- 110年桃園區網為了提升DNS的安全，與桃園市網中心合作，主動協助桃園市私立高中職學校DNS伺服器向上集中。
- 111年3月28日完成最後兩所高中職DNS向上集中，在9個月內完成全部14所私立高中職向上集中作業。



高中職 DNS 向上集中(2)

□ DNS向上集中優點

- ✓ 減少高中職學校建置管理DNS系統維護成本。
- ✓ 完成DNSSEC簽署及RPZ設定，增加了DNS服務安全性。
- ✓ 達成環保節能減碳，減少14所學校共16台 DNS 伺服器的能源消耗。

序	學校	DNS集中完成日期
1	大華高中 thsh	110/07/30
2	六和高中 lhvs	110/08/10
3	清華高中 chvs	110/08/16
4	振聲高中 fxsh	110/08/17
5	治平高中 cpshs	110/08/19
6	復旦高中 fdhs	110/08/30
7	永平工商 ypvs	110/08/31

序	學校	DNS集中完成日期
8	新興高中 hshs	110/08/31
9	啟英高中 cyvs	110/08/31
10	至善高中 tzsavs	110/08/31
11	大興高中 dxhs	110/10/13
12	桃園美國學校	111/1/14
13	方曙商工 fsvs	111/3/28
14	成功工商 ckvs	111/3/28

積極協助大專院校 DNS bind版本更新(1)

- ❑ 第一種協助作法，請連線學校提供作業系統版本，區網提供明確的bind 升級指令步驟，協助 step by step 完成升級。



柯皓翔

寄給 王得智、anping、陳姿吟、wenhou、Shih-chun、林文漢 ▼

王老師您好，

謝謝您的回覆，根據貴校作業系統版本，DNS Bind 的升級步驟如下：

1. <http://www.isc.org/downloads/> 下載軟體(以bind-9.16.33 版本為例)

2. ftp至dns主機

3. tar -xvf bind-9.16.33.tar.gz

cd bind-9.16.33

./configure (以一般user身分)

make

sudo -s

make install

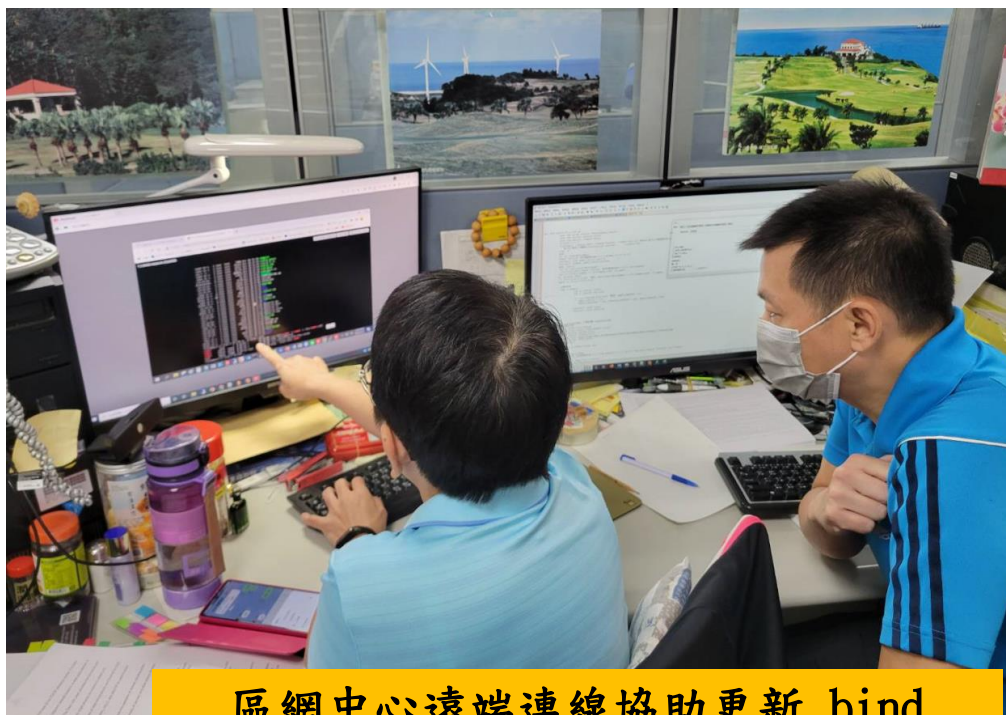
ps -ef|grep named

kill -9 xxx

/usr/local/sbin/named -c /etc/named.conf -u named

積極協助大專院校 DNS bind版本更新(2)

- ❑ 第二種協助作法，如果不熟悉bind編譯升級，或擔心影響正在上線的DNS服務，由桃園區網中心遠端連線協助編譯安裝最新之bind版本。
- ✓ 111/10/26 遠端連線協助中原大學bind更新。
- ✓ 111/10/28 遠端連線協助萬能科大bind更新。
- ✓ 111/11/03 遠端連線協助開南大學bind更新(該校FreeBSD版本老舊，當天無法完成更新bind，預計11月底該校提供新機，預計12月可完成安裝)



區網中心遠端連線協助更新 bind

桃園區網連線單位 DNS 更新進度

連線單位	單位數	已更新至最新版本	最新版本比率
縣市網中心	3	3	100%
大專院校	14	12	85%
高中職	18	全部向上集中	100%

- ❑ 遠端連線協助開南大學bind更新，但該校FreeBSD版本老舊，11/3當天無法完成更新bind，預計11月底該校提供新機，預計12月底前可完成安裝。
- ❑ 銘傳大學桃園校區尚未升級至BIND 9.16，原因為該校台北校區及桃園校區DNS架構重新調整，不方便由區網中心遠端協助，但會在12月中旬前進行更新，年底前可望完成所有連線單位bind版本100% 更新。

協助縣市網中心進行頻寬提升作業

- ❑ 配合教育部「111年度臺灣學術網路(TANet)國內骨幹(縣市)電路租用服務案」機房會勘、進線(建置)。
- ❑ 111/06/01 協助桃園市網中心頻寬提升至40G，10/13頻寬提升至60G。
- ❑ 111/08/30 協助連江縣網中心頻寬提升至2G。
- ❑ 111/08/30 協助金門縣網中心頻寬提升至2G。

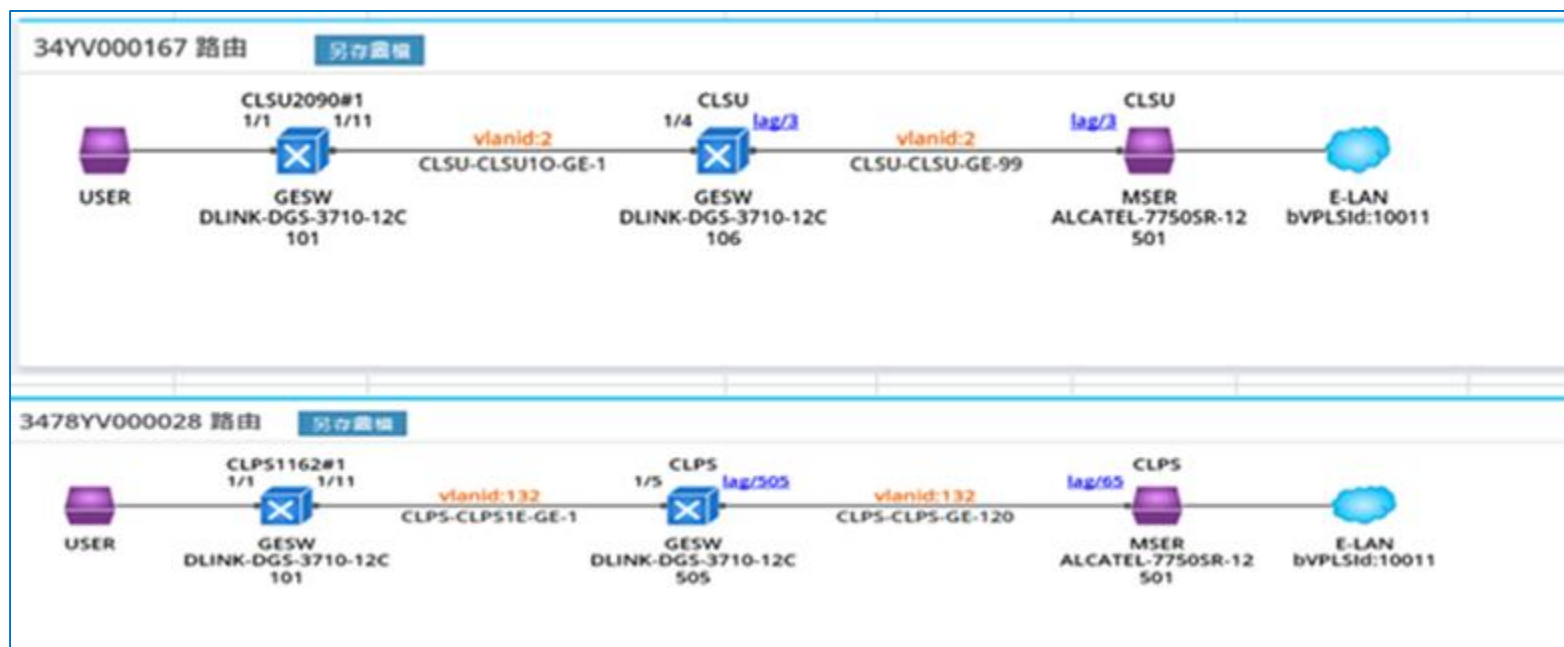
積極導入IPv6(1)

- 109年協助4所學校導入IPv6，110年協助4所學校完成IPv6。
- 但111年有4所高中完成設定後，卻無法完成IPv6連線。111年6月17日桃園區網為積極協助解決連線學校IPv6 設定問題，在陳奕明主任帶領下，拜會中華電信蘇振乾總經理、網路維運中心吳家伸主任，請該公司全力協助。



積極導入IPv6(2)

- ❑ 最後查出原因：各高中職連線桃園區網時，中華電信採E-LAN 架構，在CHT MSER網路設備啟動PBB及B-VPLS，其中B-VPLS中的MRP(MAC Registration Protocol)設定不完整，影響IPv6網路服務正常運作。



積極導入IPv6(3)

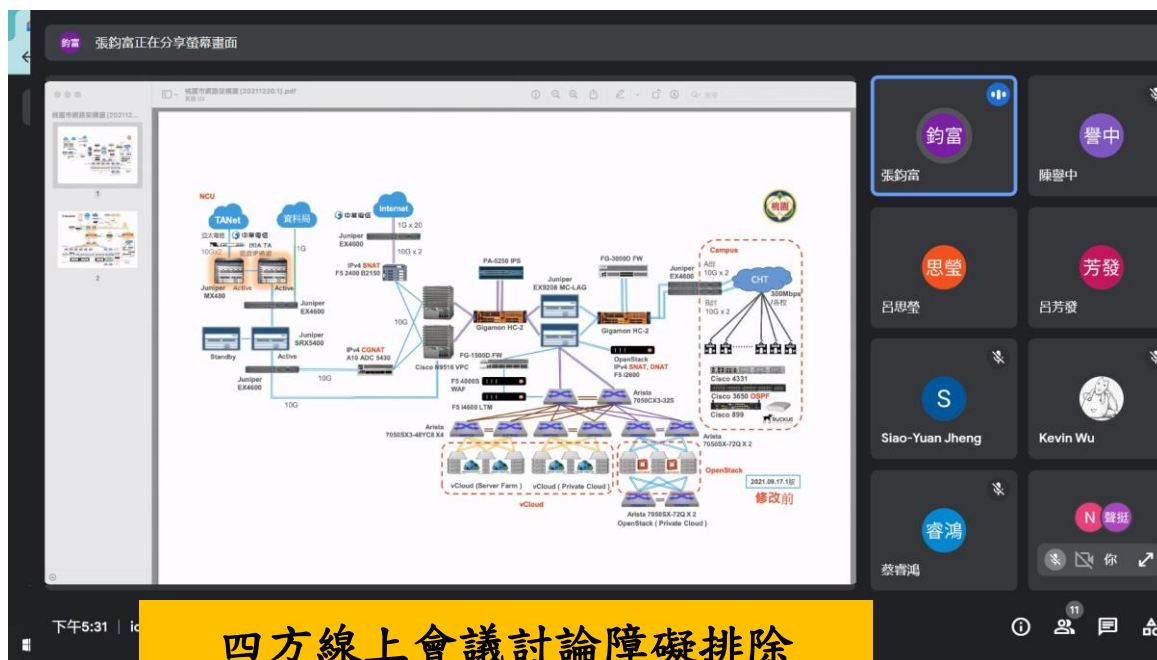
- 109年協助4所學校導入IPv6，110年協助4所學校完成IPv6。
- 111年協助治平高中、振聲高中、大華高中、復旦中學、大興高中、清華高中等6所高中導入IPv6。
- 最後5所尚未導入IPv6學校
 1. 永平工商、成功工商新接任老師，未能找到路由器帳號密碼，暫時無法導入，預計由區網中心協助進入console port重新 reset 帳密後再進行導入 IPv6 。
 2. 方曙高中、懷恩高中、至善高中3所高中路由設備不支援IPv6，無法導入 IPv6 。

積極導入IPv6(4)

連線單位	單位數	完成IPv6 單位數	未完成IPv6 單位數	完成IPv6 比率
縣市網中心	3	3		100%
大專院校	14	14		100%
高中職	18	13	5 (含3所高中路由 設備無法支援v6)	72%
總計	35	30	5	85%

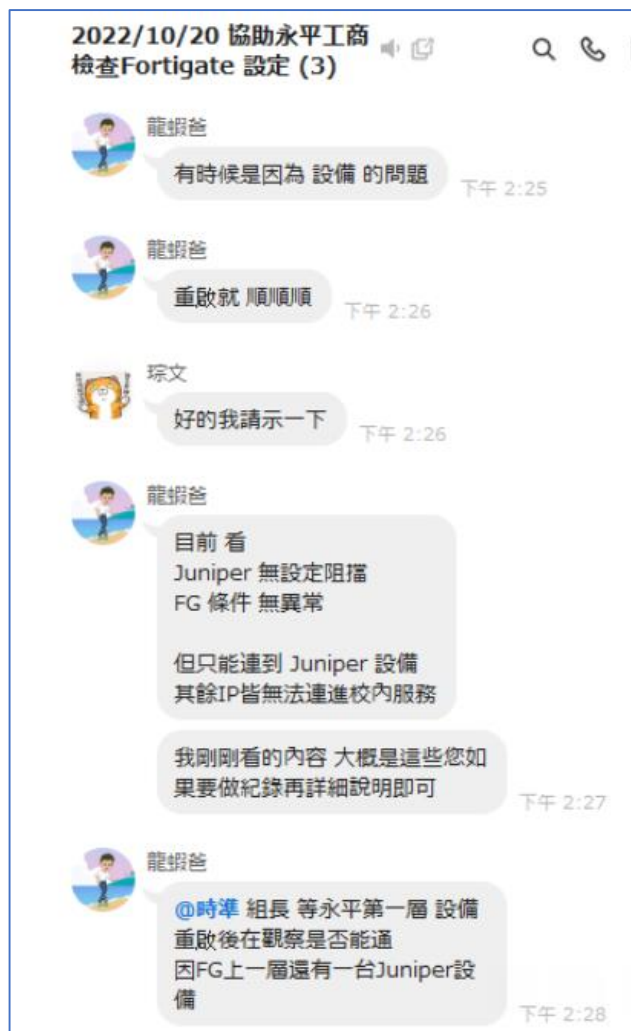
網路的障礙排除

- ❑ 桃園區網中心導入開源Zabbix系統，監測重要網路設備及線路，以確保網路及機房設備全年無休的正常運作。
- ❑ 今年協助連線學校網路的障礙排除及諮詢 總計41件。
- ❑ 以111/4/12為例，桃園市網中心反映網路連線緩慢，立即展開四方線上會議(教育部資科司、桃園區網、桃園市網、廠商)共同討論找出可能之連線問題。



四方線上會議討論障礙排除

借重連線學校夥伴的技術與經驗

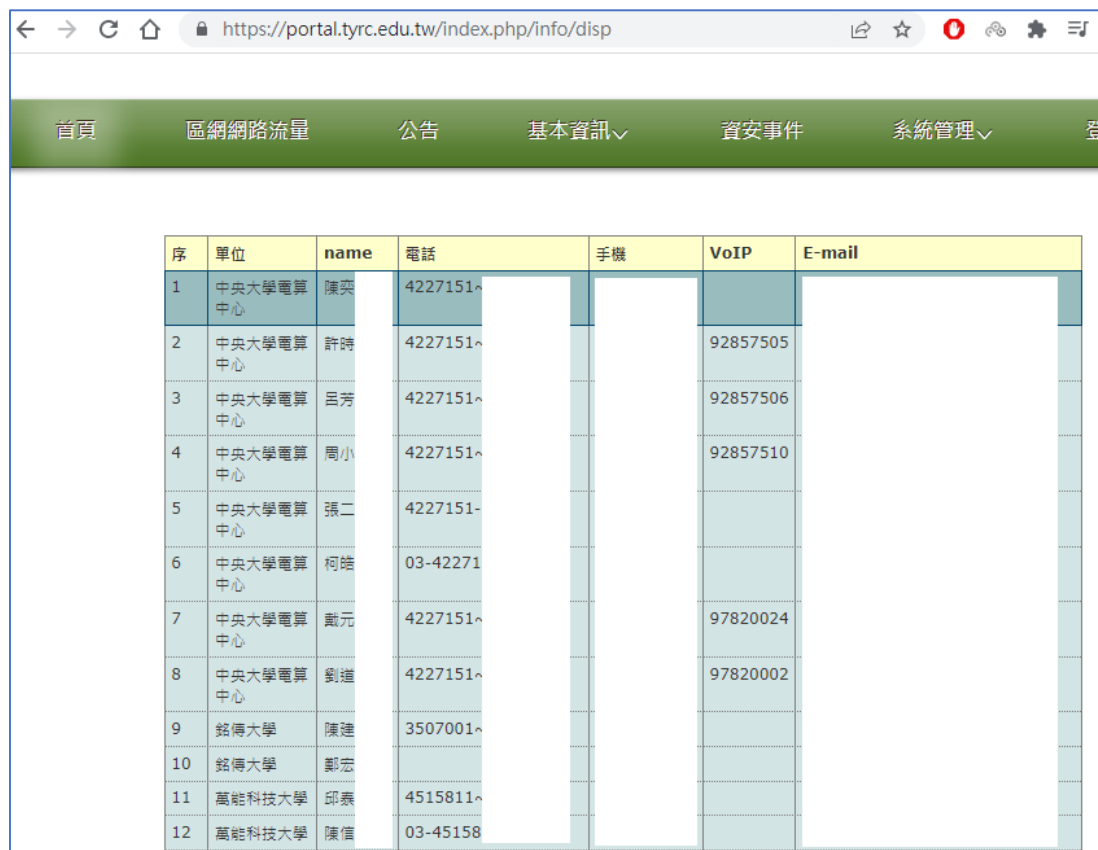


- ❑ 連線學校是區網的關鍵合作夥伴，他們的智慧(技術與經驗)是區網中心的珍貴經驗寶庫。
- ❑ 今年首度邀請有熱忱的連線學校夥伴共同查修其他學校的問題，以111/10/20為例，永平工商反映無法從外部連線該校網站。
- ❑ 桃園區網檢查憑證代理伺服器正常，但無法trace到該校內部網站，原因可能在於該校防火牆設定。
- ❑ 線上立即尋求熟悉Fortigate 設備的區網夥伴，熱心的六和高中謝勝任老師與永平工商老師、桃園區網展開三方線上會議查找障礙，經過2小時找出防火牆設定的錯誤，修正後，順利從外部連上該校網站。

區網中心、六和高中、永平工商
三方線上會議協助永平工商障礙排除

建立連線學校人員聯繫管道

- ❑ 建置桃園區網portal管理系統，建立所有連線學校相關人員聯繫資料，並依個資法簽署個資蒐集聲明書。
- ❑ 成立桃園區網LINE群組，可即時聯繫連線學校相關人員。



The screenshot shows a web browser window with the URL <https://portal.tyrc.edu.tw/index.php/info/dis>. The page has a green navigation bar with links: 首頁, 區網網路流量, 公告, 基本資訊, 資安事件, 系統管理, and 登. Below the navigation bar is a table with contact information for various institutions.

序	單位	name	電話	手機	VoIP	E-mail
1	中央大學電算中心	陳奕	4227151~			
2	中央大學電算中心	許詩	4227151~		92857505	
3	中央大學電算中心	呂芳	4227151~		92857506	
4	中央大學電算中心	周小	4227151~		92857510	
5	中央大學電算中心	張二	4227151-			
6	中央大學電算中心	柯皓	03-42271			
7	中央大學電算中心	戴元	4227151~		97820024	
8	中央大學電算中心	劉道	4227151~		97820002	
9	銘傳大學	陳建	3507001~			
10	銘傳大學	鄭宏				
11	高能科技大學	邱泰	4515811~			
12	高能科技大學	陳信	03-45158			

建置區網網站常見問題FAQ

- ❑ 以使用者為中心提供更友善的介面與服務，建立網管、資安技術、教育訓練、DNS升級問題集FAQ，供連線學校查詢，可提供連線學校老師先自行排除問題，並節省區網人員回覆問題的工作量。



The screenshot shows a web browser window with the URL <https://www.tyrc.edu.tw>. The page title is "桃園區域網路中心" (Taoyuan Regional Network Center). The navigation menu includes "關於桃園區網", "特色服務", "網路流量", "會議資料", "教育訓練", "資安服務", and "FAQ". The "FAQ" link is circled in blue. The main content area is titled "DNS升級FAQ" and contains two questions and answers:

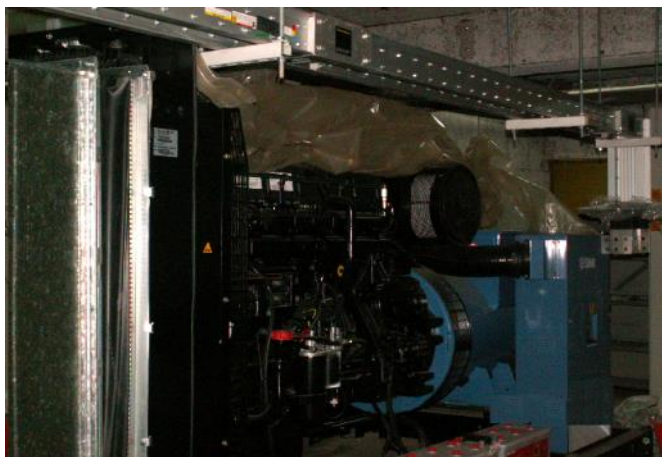
- Q 1 : CentOS , DNS Bind 的升級步驟 ?
A :
1. 下載軟體(以bind-9.16.33 版本為例)<https://isc.org/download/>
2. ftp至dns主機。
3. tar -xvf bind-9.16.33.tar.gz
./configure (以一般user身分)
make。
sudo -s
make install
ps -ef|grep named
kill -9 xxx
/usr/local/sbin/named -c /etc/named.conf -u named
如果系統有少裝的套件，則要視情況處理。
- Q 2 : FreeBSD , DNS Bind 的升級步驟 ?

A sidebar on the right contains a list of links: "網管類", "資安類", "教育訓練", "DNS升級" (highlighted in green), "※異地備份服務", "※綜合服務申請", and "※個資蒐集聲明".

<https://www.tyrc.edu.tw/>

機房電力、空調、溫溼度

- 持續機房維運建設(電力、空調), 維持良好網路運作
 - 具450KVA發電機組及500KVA發電機組共2座。
 - 模組式UPS, 200K-A, 200K-B, 並具備切換二部發電機之開關
 - 10噸x3+1台窗型冷氣空調系統
 - 網路溫/濕度計, 建置機房溫度/濕度監看網頁



桃園區網維運—機房管理

- ❑ 訊息公告，重要訊息並以Email寄送、LINE公告至各連線單位
- ❑ 機房工作日誌


桃園區域網路中心

[關於桃園區網](#)
[特色服務](#)
[網路流量](#)
[會議資料](#)
[教育訓練](#)
[資安服務](#)
[FAQ](#)

桃園區網中心

Taoyuan Network Regional Center

【年度執行成效首頁】

桃園區網中心地址：(32001) 桃園市中壢區中大道300號-志希館1 F
週一至週五：8-17時 電話：03-4227151 (分機轉 57555/57566)
週一至週五：17-22時 電話：03-4227151 (分機轉 57511)
電子信箱：tanet_ncu@ncu.edu.tw

公告時間	標題	公告內容	網址	附件
2022-10-17 10:58:28	[訊息轉發]【資安訊息】請各單位加強留意DDOS「分散式阻斷服務攻擊」及偽冒技服中心名義之「資通安全協置函」釣魚信件	教育機構ANA通報平台 發佈編號 TACERT-ANA-202210170 詳見全文		
2022-10-07 13:38:10	[訊息轉發]【漏洞預警】微軟Microsoft Exchange Server存在安全漏洞(CVE-2022-41040與CVE-2022-41082)，允許攻擊者遠端執行任意程式碼，請速確認並評估採取緩解措施	教育機構ANA通報平台 發佈編號 TACERT-ANA-202210071 詳見全文		

維護編號	維護事項	維護日期	更新	刪除
TWAREN20220919-1	TWAREN SDN 設備檢查/保養	2022-09-19		
TWAREN20220803-1	TWAREN 主機檢查/保養	2022-08-03		
TWAREN20220712-1	TWAREN N5K網維升級	2022-07-12		
TWAREN20220617-1	TWAREN SDN 設備檢查/保養	2022-06-17		
TANET20220512-4	TANet 100G-電池主機維護/保養	2022-05-12		
TANET20220512-3	TANet 100G-SMR主機維護/保養	2022-05-12		
TANET20220512-2	TANet 100G-RPM主機維護/保養	2022-05-12		
TANET20220512-1	TANet 100G主機維護/保養	2022-05-12		
TWAREN20220512-1	TWAREN 100G 主機維護/保養	2022-05-12		
TWAREN20220310-1	TWAREN SDN 設備檢查/保養	2022-03-10		
TWAREN20220217-1	TWAREN 100G 主機維護/保養	2022-02-17		
TANET20220217-4	TANet 100G-電池主機維護/保養	2022-02-17		
TANET20220217-3	TANet 100G-SMR主機維護/保養	2022-02-17		
TANET20220217-2	TANet 100G-RPM主機維護/保養	2022-02-17		
TANET20220217-1	TANet 100G主機維護/保養	2022-02-17		
TWAREN20220215-1	TWAREN 主機檢查/保養	2022-02-15		

桃園區網管理委員會(1)

- ❑ 管理委員會每半年召開一次，並輪流到各連線學校開會，達到觀摩交流之目的。
- ❑ 111年5月4日因疫情影響，第69次會議改為線上會議，連線單位出席率89%。
 - ✓ 資安宣導及業務報告
 - ✓ 核能研究所、中壢高中及元智大學老師經驗分享

錄製中 | 核研所Tseng正在分享螢幕畫面

核研所的資訊安全管理

ISMS內稽、外稽
政風資安稽核
職安會資訊稽核

宣導 行動 稽核

- 導入最新版本ISMS (ISO:27001:2013)
- 動Windows作業系統更新
- 電腦全面安裝防毒軟體
- 定期更新防毒軟體資料庫
- 導入XDR
- 資通安全威脅偵測管理，以Splunk持續監控中
- 持續佈署政府組態基準
- 弱點掃描，每月一次
- 滲透測試，排定於ISMS中委外辦理
- 導入Vans (資通安全弱點通報機制)
- 資通安全防護

社交工程
資安政策
教育訓練

還有另外 32 位使用者

上午10:27 | vso-bzve-tie

40

桃園區網管理委員會(2)

- 111年10月6日於中原大學召開第70次會議，會議採實體及視訊會議並行，連線單位出席率91%(現場人數+線上人數)。
 - ✓ 資安宣導及業務報告
 - ✓ 第三屆傑出網管人員頒獎
 - ✓ 第四屆傑出網管人員選拔
 - ✓ 楊梅高中老師經驗分享



桃園區網第四屆傑出網路管理人員選拔

□ 2022/10/6 桃園區網第四屆傑出網路管理人員選拔，當選人如下

- ✓ 金門縣教育網路中心 謝維倫組長
- ✓ 桃園市福豐國中 李勁緯組長
- ✓ 元智大學 羅紀斌技佐
- ✓ 金門縣教育網路中心 王哲剛組長



桃園區網LINE群組

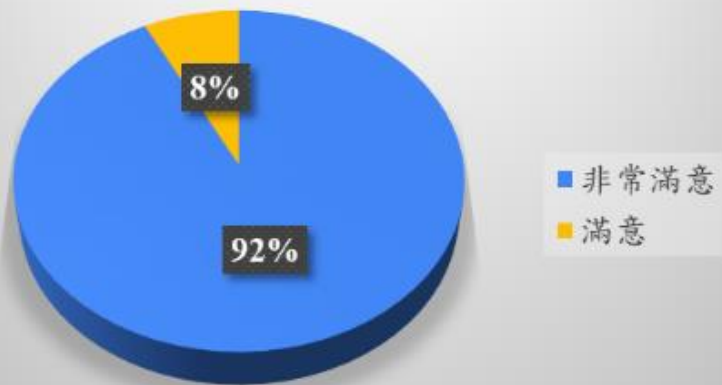
- ❑ 網路連線問題的即時發現與處理
- ❑ 病毒或網路攻擊訊息的即時分享
- ❑ 連線學校間的經驗分享平台與互相查找問題



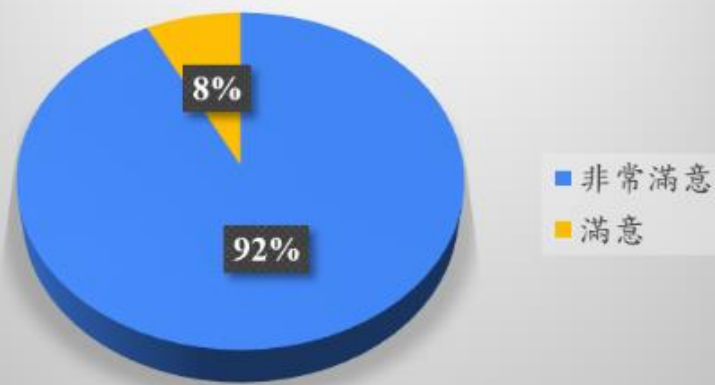
服務滿意度調查

- 填寫問卷學校：40所

貴單位對於區網中心處理問題的速度與回應是否滿意？



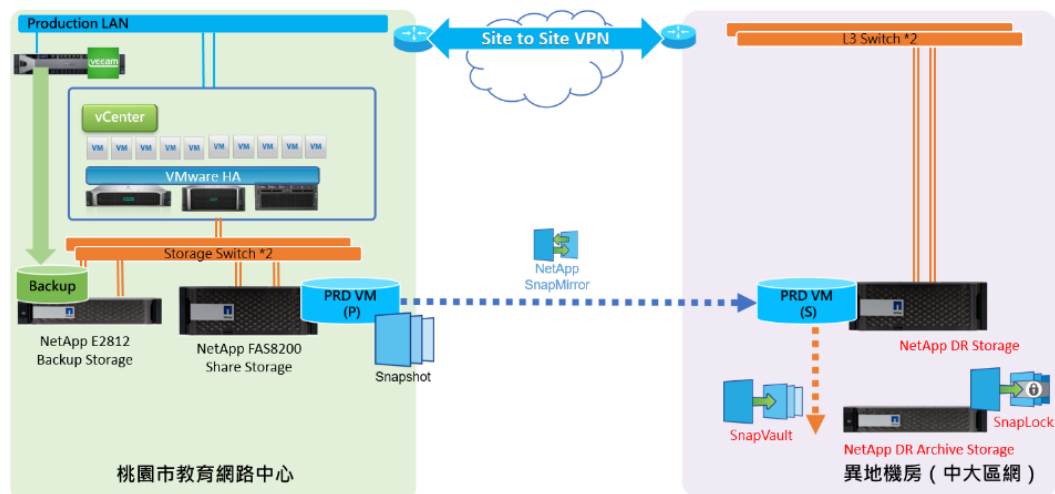
貴單位對於區網中心整體服務是否滿意？



加強與縣市網中心合作

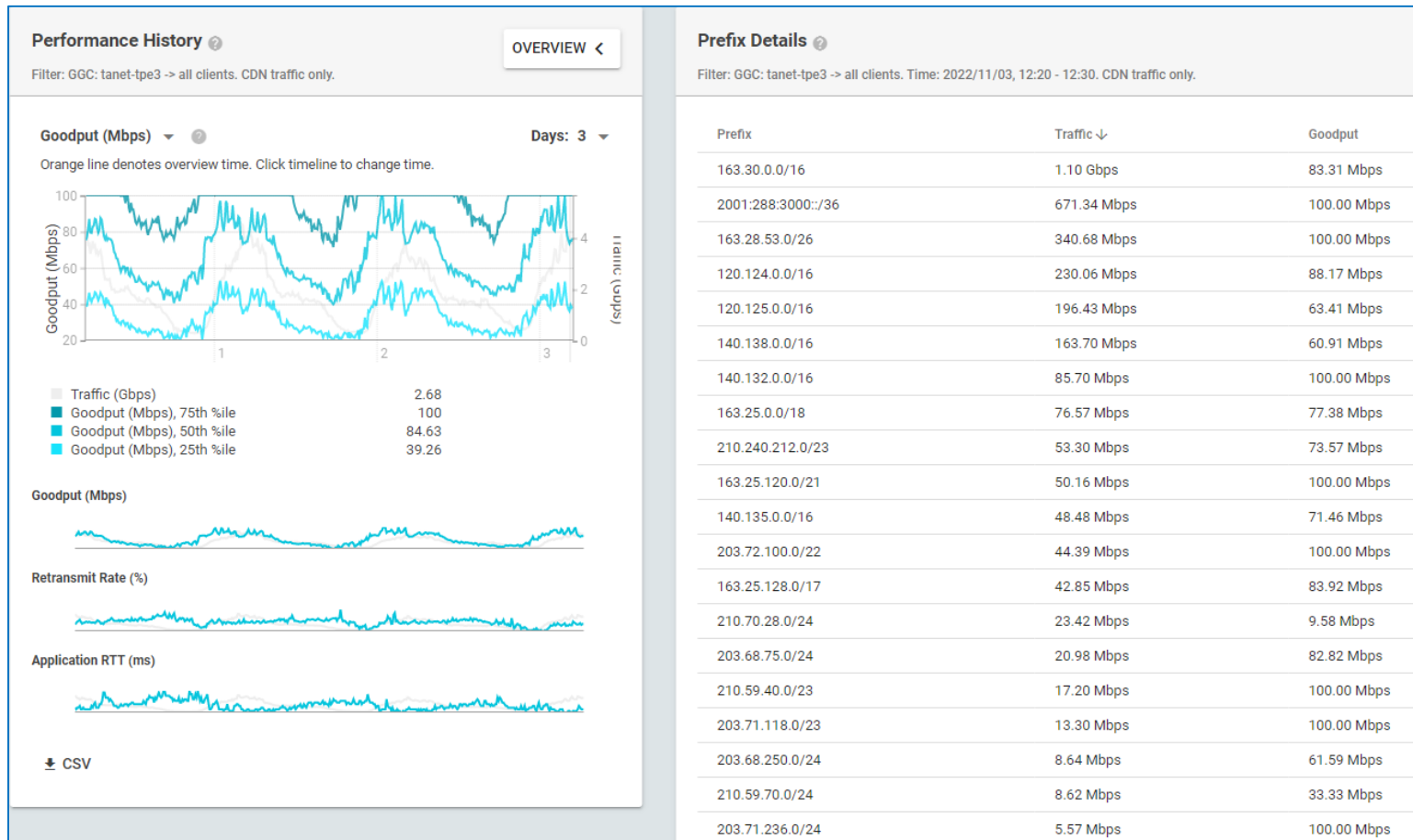
- 110~111年與桃園市網中心合作，協助14所私立高中職學校DNS伺服器向上集中，達成提升DNS安全性及減少人力維護成本，並同時完成DNSSEC簽署及RPZ設定。
- 111年4月14日與桃園市網中心洽談異地備份、異地備援。
- 111年12月8日與連江縣網中心合作，針對其需求進行手把手的實作教學，辦理資訊安全管理系統導入、機房管理訪視與網路巡檢。

異地備份架構圖 Phase I



GGC新節點 111/9/30 正式上線

GGC 新節點 2xDell R740xd + Cisco 5001 完成硬體安裝及架設線路，並於9/30正式上線提供服務，舊GGC node 於10/7下線停止服務。



導入Eduroam進度

- 111年協助新生醫護管理專科學校、健行科大、國立體育大學，完成eduroam無線漫遊建置。
- 111年3月22日邀請無線網路漫遊中心張家倫先生講授eduroam無線漫遊建置。
- 111年10月6日並於區網會議宣導，目前僅支援TANetRoaming 無線漫遊之學校，提請規劃推動期程及需要設備，完成轉換至eduroam無線漫遊。

桃園區網導入Eduroam進度

連線單位	單位數	已導入 Eduroam	僅有 TANetRoaming	兩者皆無
縣市網中心	3	3		
大專院校	14	8	4	2
高中職	18	3	1	14
總計	35	14	5	16



第三章



資安服務

資安巡迴服務

協助連線學校檢視資安防護能力

協助檢視網路架構及網路活動

提供連線學校資安改善建議

提供連線學校到點服務

■ 執行資安巡迴服務同仁之專業證照

ISO27001	CHFI	CND	CCNA	CEH	CISSP	CCSK
3張	2張	1張	1張	1張	1張	2張

資安巡迴執行時程

111/6 開始，每季接受一所連線學校申請資安巡迴服務



依照申請送出順序及緊急程度，排程完成巡迴服務



服務以遠距執行及到點服務並行，
到點服務，以一日內可完成之服務
為原則。

111/07/14 至振聲中學資安巡迴服務



項次	項目	數量
1	伺服器主機檢測	學校官網www.fxsh.tyc.edu.tw i.fxsh.tyc.edu.tw、igt.fxsh.tyc.edu.tw、 fxshap.fxsh.tyc.edu.tw、會計系統、健康系統
2	物聯網設備檢測	網路印表機、事務機、門禁讀卡機
3	防火牆設置、 網路架構檢測	規劃 Server Farm專用網段，內部使用者區域中也 限制存取伺服器的特定服務，不能直接 SSH或遠端 桌面伺服器。

桃園區網提供的資安檢測(1)

- 桃園區域網路中心每年提供2次（上半年及下半年）資安檢測服務
 - 網頁檢測(Web)使用HCL APP Scan檢測
 - 弱點掃描(IP)使用Tenable Nessus Professional做為檢測工具。
- 定期追蹤申請單位是否針對弱點結果修正，修正後會再次執行掃描以確保弱點是否已修復。
- 總計協助8所學校申請弱點掃描472個主機，網頁檢測54個網站。

申請學校	弱點掃描	網頁檢測	追蹤處理情形
桃園市龍潭高中	1	3	2022/03/15追蹤
中央警察大學	3	4	2022/03/15追蹤
國立體育大學	53	2	2022/03/15追蹤
南亞技術學院	5	6	2022/03/15追蹤
元智大學	27	3	2022/03/15追蹤
中原大學	31	12	2022/03/15追蹤

桃園區網提供的資安檢測(2)

申請學校	弱點掃描	網頁檢測	追蹤處理情形
桃園市龍潭高中	3	2	2022/09/15追蹤
中央警察大學	4	5	2022/09/15追蹤
萬能科技大學	3	1	2022/09/15追蹤
國立體育大學	256	5	2022/09/15追蹤
中央大學	53	0	2022/09/15追蹤
中原大學	33	11	2022/09/15追蹤
總 量	472	54	已全數追蹤

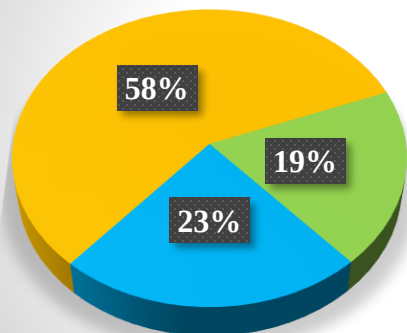
桃園區網提供的資安檢測(3)

□ 系統弱掃概況

➤ 系統弱掃工具：Nessus Professional

統計日期	總系統數	高風險系統數	中風險系統數	低風險系統數	未發現風險系統數
111/3/15	123	18	28	2	72
111/9/15	295	29	20	0	246
111/10/24 (復掃結果)	291	17	32	0	242

系統弱掃中高風險修補情形追蹤



■ 已預計修補時程
■ 接受風險
■ 誤報

追蹤填寫接受風險的IP
皆為中風險，且該校確
認不具立即風險。

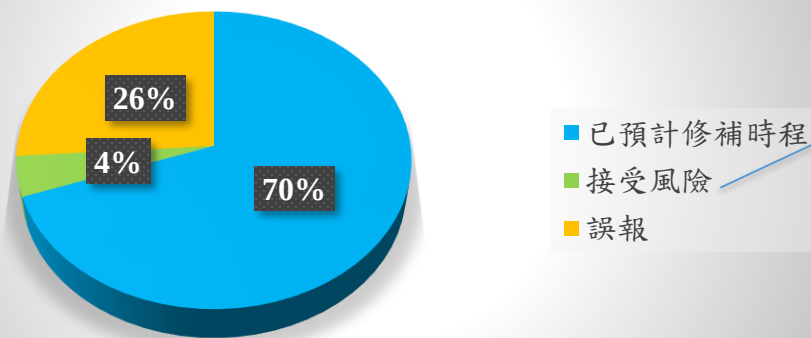
桃園區網提供的資安檢測(4)

□ 網站檢測概況

➤ 網站檢測工具：HCL AppScan

統計日期	總網站數	高風險網站數	中風險網站數	低風險網站數	未發現風險網站數
111/3/15	22	7	10	5	0
111/9/15	21	15	4	2	0
111/10/24 (復掃結果)	21	9	4	3	5

網站弱掃中高風險修補情形追蹤



追蹤填寫接受風險的網站皆為中風險，且該校確認不具立即風險。

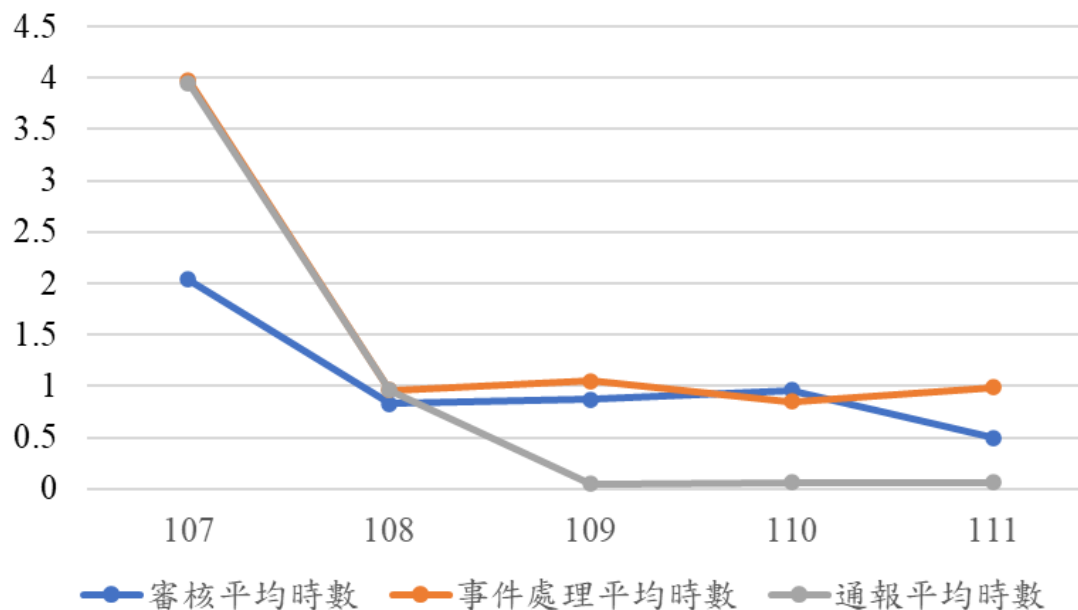
資安事件統計

資料統計：2022/1/1-2022/09/30		桃園區域網路中心
1. 1、2級資安事件處理		
(1)通報平均時數：	小時	0.06
(2)應變處理平均時數：	小時	0
(3)事件處理平均時數：	小時	0.99
(4)通報完成率：	百分比	100%
(5)事件完成率：	百分比	100%
2. 3、4級資安事件通報		無
3. 資安事件通報審核平均時數：	小時	0.5
聯絡相關資訊完整度：	百分比	74.07%

去年100%，但今年開始加填資安長，部分學校漏填，已全數追蹤補填完畢。

歷年資安事件處理平均時數

桃園區域網路中心1、2級資安事件處理平均時數

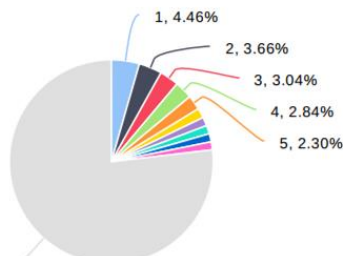


年度	107	108	109	110	111
審核平均時數	2.04	0.829	0.87	0.96	0.5
事件處理平均時數	3.98	0.961	1.05	0.85	0.99
通報平均時數	3.95	0.96	0.05	0.06	0.06

資安服務—Top流量

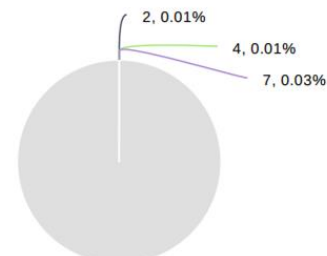
Top 200 Byte

2022/10/13 00:00 ~ 2022/10/13 23:59



Top 200 Session

2022/10/13 00:00 ~ 2022/10/13 23:59



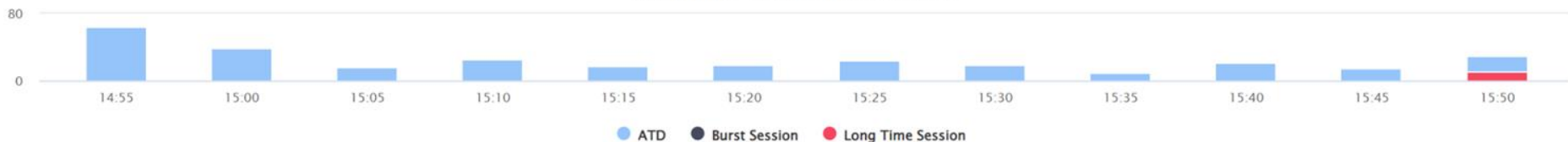
總筆數200

no	來源 IP	來源 IP 名稱解析	次數	Session	Packet	byte
1	140.115.145.143	中央大學	0 / 0	2.95K / 887.36M	558.50M / 40.65G	808.10G / 18137.96G 4.46%
2	203.71.101.1	治平中學	0 / 0	76.57K / 887.36M	469.95M / 40.65G	663.53G / 18137.96G 3.66%
3	163.30.93.19	桃園市網	0 / 0	8.82K / 887.36M	387.36M / 40.65G	550.61G / 18137.96G 3.04%
4	163.30.203.2	桃園市網	0 / 0	65.84K / 887.36M	1.07G / 40.65G	515.71G / 18137.96G 2.84%
5	2001: 288: 3001: 50: d8c5: d593: ad60: 3475	中央大學	0 / 0	6.51K / 887.36M	477.42M / 40.65G	417.31G / 18137.96G 2.3%
6	192.83.181.65	體育大學	0 / 0	6.66K / 887.36M	193.67M / 40.65G	282.54G / 18137.96G 1.56%
7	203.68.250.6	桃園農工	0 / 0	271.80K / 887.36M	269.66M / 40.65G	250.07G / 18137.96G 1.38%
8	203.68.249.200	新興工商	0 / 0	544 / 887.36M	184.80M / 40.65G	240.37G / 18137.96G 1.33%
9	120.125.200.64	Home	0 / 0	11.73K / 887.36M	164.93M / 40.65G	234.53G / 18137.96G 1.29%
10	2001: 288: 3014: 2: : 200	新興工商	0 / 0	344 / 887.36M	172.37M / 40.65G	227.62G / 18137.96G 1.25%
11	140.138.83.253	元智大學	0 / 0	64.84K / 887.36M	130.64M / 40.65G	150.88G / 18137.96G 0.83%
12	163.30.116.64	桃園市網	0 / 0	30.57K / 887.36M	99.16M / 40.65G	140.74G / 18137.96G 0.78%
13	2001: 288: 3200: 8: 268: 200: 2258: bb6	桃園市網	0 / 0	5.81K / 887.36M	107.98M / 40.65G	136.02G / 18137.96G 0.75%
14	192.192.227.92	tyrc_svr	0 / 0	10.47K / 887.36M	303.48M / 40.65G	135.82G / 18137.96G 0.75%
15	2001: 288: 3200: 8: 268: 200: 8139: 120c	桃園市網	0 / 0	2.77K / 887.36M	94.55M / 40.65G	118.66G / 18137.96G 0.65%
16	210.70.28.96	武陵高中	0 / 0	614.74K / 887.36M	100.28M / 40.65G	115.43G / 18137.96G 0.64%
17	163.30.105.6	桃園市網	0 / 0	3.49M / 887.36M	204.47M / 40.65G	110.32G / 18137.96G 0.61%
18	163.25.24.20	連江縣網中心	0 / 0	5.97K / 887.36M	83.14M / 40.65G	93.62G / 18137.96G 0.52%
19	163.25.121.206	金門縣網中心	0 / 0	6.34K / 887.36M	72.94M / 40.65G	85.58G / 18137.96G 0.47%

資安服務—異常流量告警

Flow ATD 即時趨勢分布圖

2022/10/14 14:58 ~ 2022/10/14 15:58 (time unit: 5mins)



IP 範圍:

3D Globe

異常項目	攻擊者 IP	攻擊者區域	受害者 IP	受害者區域	協定	目的 Port	Session	Packet	Byte	開始時間	結束時間	瀏覽
TCP SYN Host Scan	45.93.16.71	US			TCP	5038	273.78K	276.64K	14.59M	2022/10/14 14:59	2022/10/14 15:56	
TCP SYN Host Scan	165.232.190.166	IN			TCP	2009	71.54K	71.54K	3.77M	2022/10/14 15:00	2022/10/14 15:56	
TCP SYN Host Scan	146.19.191.117	DE			TCP	23	124.3K	124.3K	6.55M	2022/10/14 15:26	2022/10/14 15:56	
TCP SYN Host Scan	143.110.178.114	IN			TCP	2005	160.59K	160.59K	8.47M	2022/10/14 14:59	2022/10/14 15:56	
TCP SYN Host Scan	150.158.91.148	CN			TCP	6379	172.17K	172.17K	12.44M	2022/10/14 15:17	2022/10/14 15:56	
TCP SYN Host Scan	165.22.215.149	IN			TCP	2019	178.29K	178.29K	9.4M	2022/10/14 14:59	2022/10/14 15:56	
TCP SYN Host Scan	134.209.156.22	IN			TCP	2004	161.69K	161.69K	8.53M	2022/10/14 14:59	2022/10/14 15:56	
TCP SYN Host Scan	198.199.95.208	US			TCP	9000	83.36K	83.36K	4.4M	2022/10/14 15:53	2022/10/14 15:56	
Host Scan	146.88.240.4	US			UDP	5060	269.53K	269.53K	47.64M	2022/10/14 15:46	2022/10/14 15:56	
TCP SYN Host Scan	192.241.193.130	US			TCP	4848	103.69K	103.8K	5.48M	2022/10/14 15:51	2022/10/14 15:56	
TCP SYN Host Scan	173.247.227.70	US			TCP	23	23.14K	23.14K	1.22M	2022/10/14 15:28	2022/10/14 15:56	
TCP SYN Host Scan	154.89.5.68	HK			TCP	9999	124.63K	124.63K	7.06M	2022/10/14 15:03	2022/10/14 15:56	
TCP SYN Host Scan	165.22.215.169	IN			TCP	2024	177.14K	177.14K	9.34M	2022/10/14 14:59	2022/10/14 15:56	
TCP SYN Host Scan	165.232.177.129	IN			TCP	2010	54.17K	54.17K	2.86M	2022/10/14 15:27	2022/10/14 15:56	

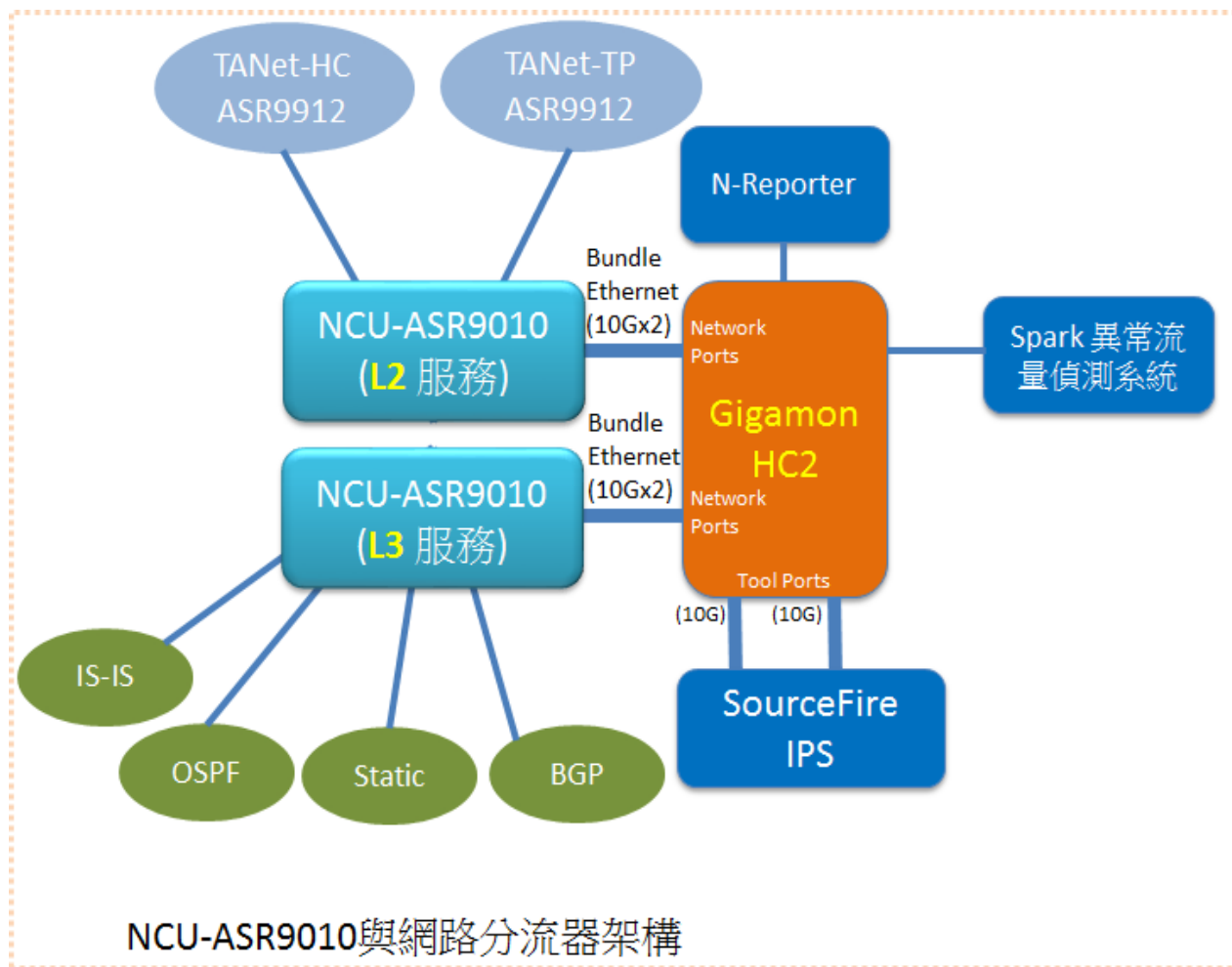
資安服務-ISMS資安認證

- 桃園區網中心(中央大學電算中心)自2010年取得ISO27001認證後，每年均依規定接受複查以保持證照有效性；2022年3月通過ISO 27001:2017 重新驗證。
- 提供桃園區域網路中心資訊安全技術相關之服務
- 轄下連線學校共有18個學校通過資安第三方認證。
- 本中心共有23張ISO 27001:2013 LA、2張CISSP、4張CEH、3張CHFI等行政院國家資通安全會報公告之專業資安證照；3張資安職能證書。

資安服務-個資保護驗證

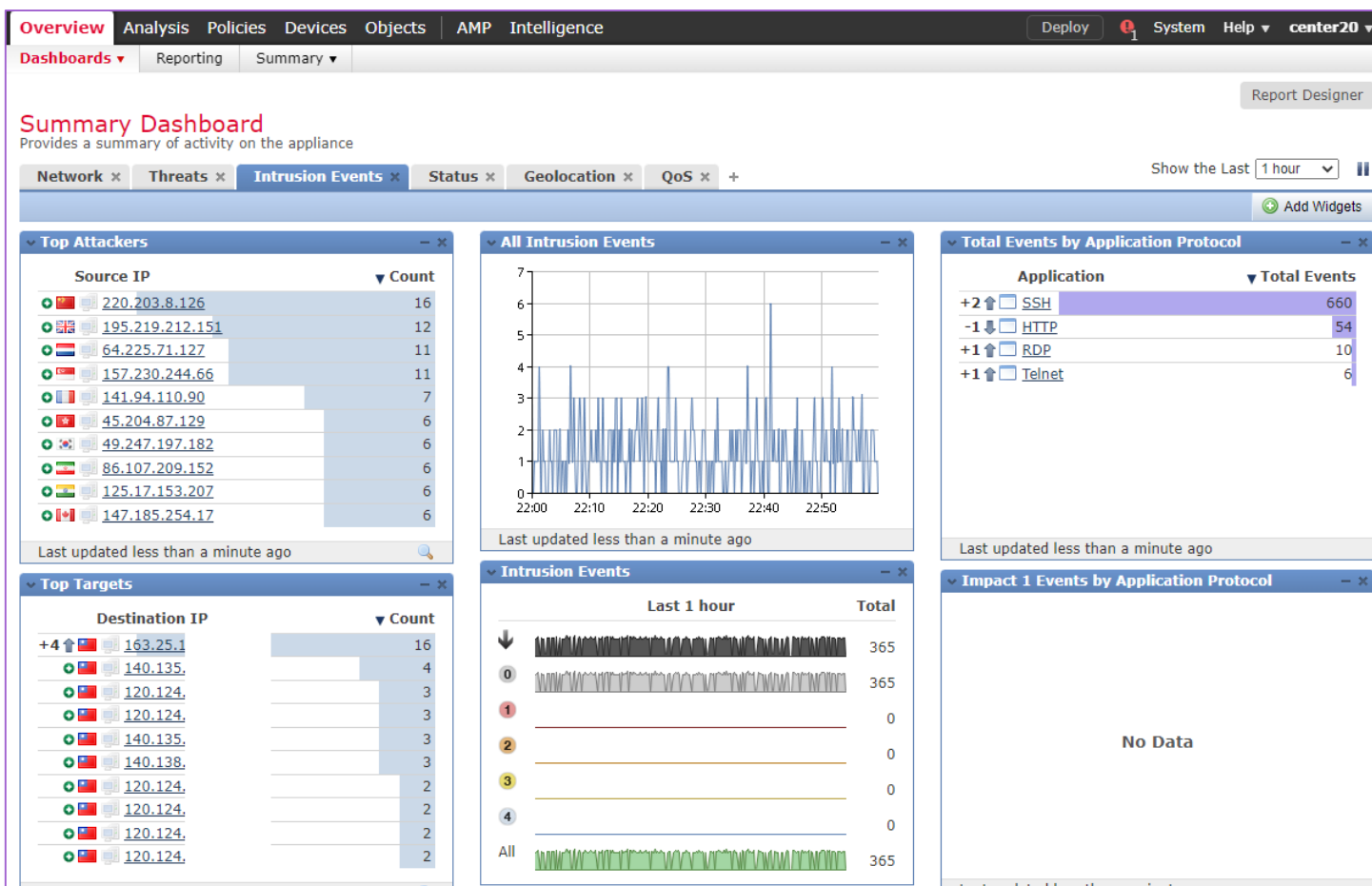
- 中央大學於106年率先通過新版教育體系資通安全暨個人資料管理規範驗證，成為國內首批通過教育體系個人資料管理規範驗證學校之一。
- 持續接受「教育機構資安驗證中心」稽核，以維持本校個人資料管理制度之有效性，於109年4月通過重新驗證，111年2月通過第二次追查稽核。
- 桃園區域網路中心提供之各項服務及填寫表單，皆依照教育體系資通安全暨個人資料管理規範執行。

桃園區網資安系統架構

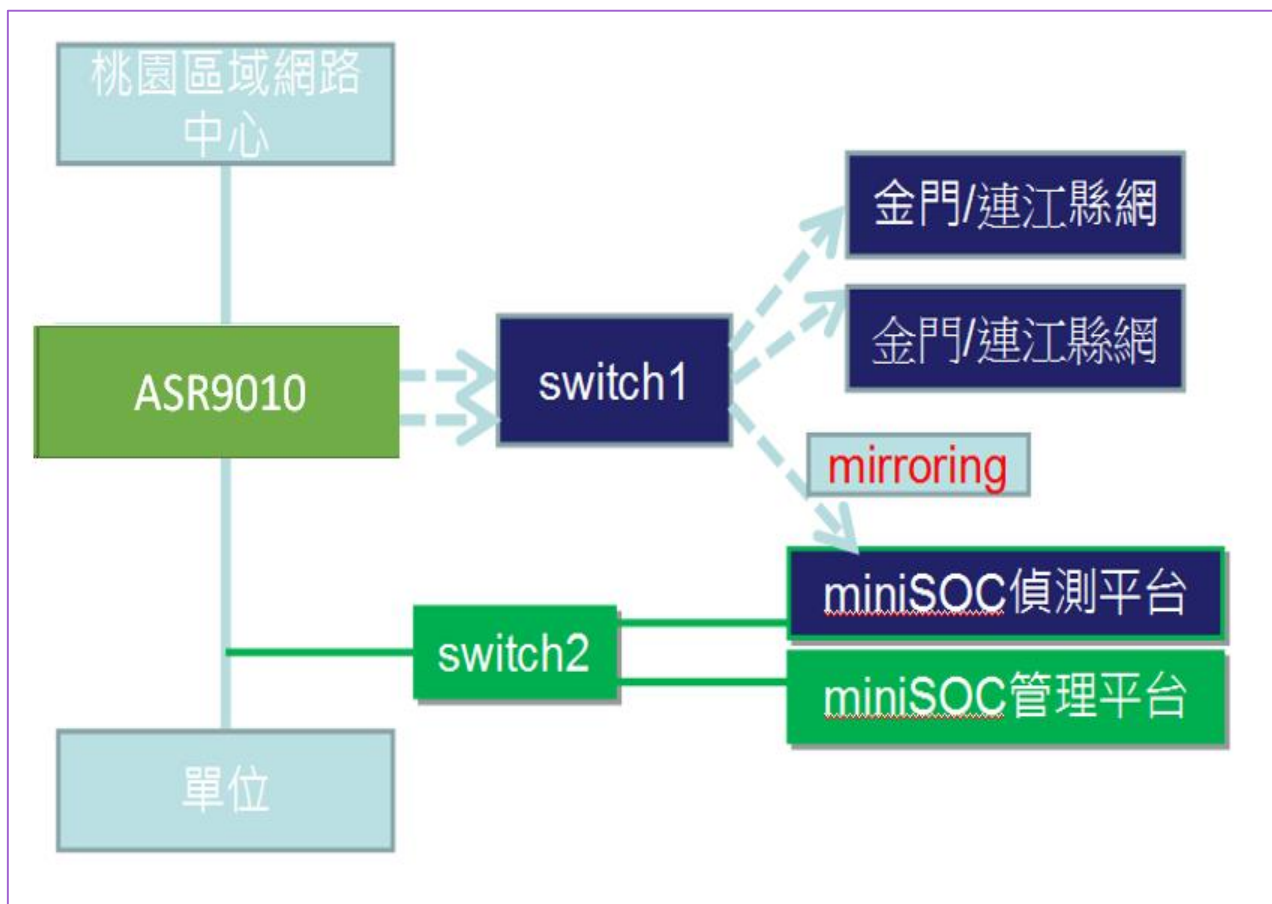


資安服務-區網入侵防禦系統

- ❑ Cisco FirePower IPS inline 運作，協助連線學校降低不當資訊的流竄、網路攻擊事件之發生，以提昇網路使用效率。



金門/連江縣網MiniSOC偵測平台

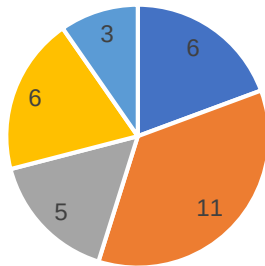


111年辦理之教育訓練

時間	主講人	課程名稱
111年03月22日	張家倫先生 東華大學臺灣學術無線網路漫遊中心	eduroam無線漫遊建置
111年05月04日	蔣懷孝老師 中原大學	IT工作壓力的調適與舒壓
111年06月15日	劉得民老師 中華民國網路封包分析協會理事長	資安線上講座「資通安全概論」
111年08月26日	張二川技正 國立中央大學電子計算機中心	資安其實很簡單
111年09月07日	蔡一郎執行長 微智安聯股份有限公司 創辦人暨執行長	勒索軟體與防治資料外洩應對指引
111年09月21日	鍾沛原專案經理 國立成功大學資通安全研究與教學中心(TWISC)	校園資安防護及資安法因應
111年10月13日	施衣喬老師 國立宜蘭大學圖書資訊館	主機滲透測試與 vulnhub 靶機初探

多元的教育訓練師資

108年~111年開課師資(總計31場)



- 區縣市網夥伴
- 資安協會及民間企業
- 教育部計畫成立之中心
- 學術單位
- 國家高速電腦中心

以108年~111年為例

舉辦31場，師資廣邀區縣市網路中心夥伴、國家高速電腦中心、教育部計畫、科技部計畫成立之中心、資安協會、民間企業等。

教育訓練師資之多元化，能以更多不同角度來闡釋資訊安全、網路管理及其他議題。

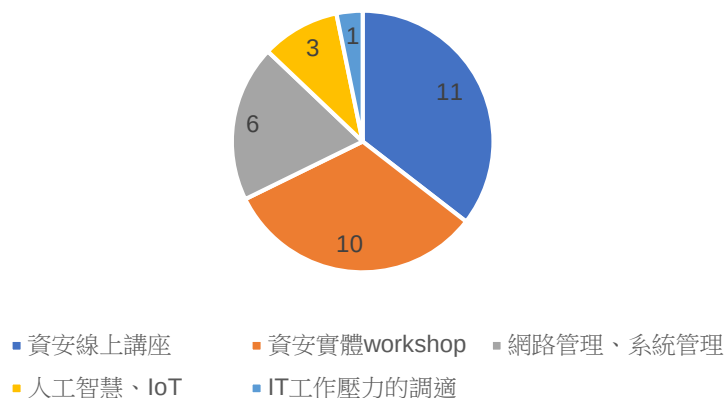
台北區網
台北第二區網
宜蘭區網
高屏澎區網
新竹縣網

北區學術資訊安全維運中心ASOC
臺灣學術網路危機處理中心TACERT
TANet 無線網路漫遊中心
資通安全研究與教學中心TWISC

政治大學
淡江大學
中原大學
中山大學
振聲高中

涵蓋多層面的教育訓練主題

108~111年教育訓練主題(總計31場)



以108年~111年為例

訓練主題以資安實作 workshop為主，受疫情影響後，改為線上課程分布資安、網路管理、系統管理，並將主題擴大至AI、IoT。

涵蓋多層面之訓練主題，並因應連線學校夥伴的需求，提供更多面向的講題，例如初探Python AI 深度學習的第一堂課、自建同步視訊教學系統、Google+Arduino+Appinventor、IT工作壓力的調適與舒壓課程等。

Workshop 第一場- 網站弱點評估實務

Workshop 第二場- 網路封包分析實務

Workshop 第三場- 源碼檢測實作

Workshop 第四場- 開源碼主從式稽核記錄系統建置

Workshop 第五場- 建置資安攻防演練平台-從原理到實作

初探 Python AI 深度學習的第一堂課

手機網路封包分析

物聯網設備資安攻防技術實務

駭客攻防於IOT與公共基礎設施

IT工作壓力的調適與舒壓

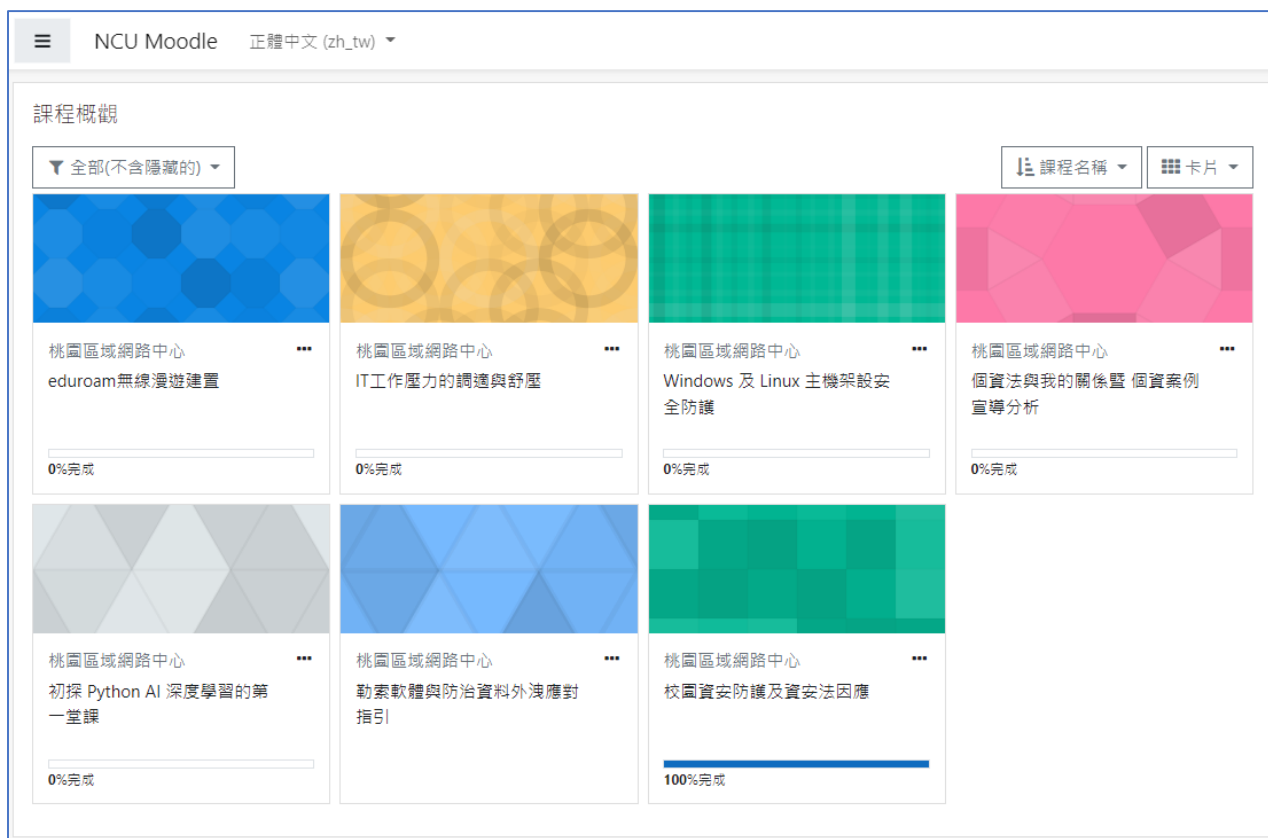
善用全球智慧—自建同步視訊教學系統

Google+Arduino+Line+ Appinventor 超乎你想像的免費工具

教育訓練數位化

桃園區網中心Moodle線上學習系統

- 1、網頁位置: <https://eustoma.cc.ncu.edu.tw/> 需註冊帳號方能使用。(另提供審查委員登入帳號)
- 3、目前可以選課的教育訓練課程點擊桃園區域網路中心進入，目前共有7門可以線上選課及提供上課影片的訓練課程，會陸續上架後續舉辦的教育訓練課程。



桃園區網Moodle線上學習系統

- 目前共有7門課提供影片可以線上選課，課程內容提供課程影音、課程講義
- ✓ 「 IT工作壓力的調適與舒壓 」
 - ✓ 「 eduroam無線漫遊建置 」
 - ✓ 「 勒索軟體與防治資料外洩應對指引 」
 - ✓ 「 校園資安防護及資安法因應 」
 - ✓ 「 初探 Python AI 深度學習的第一堂課 」
 - ✓ 「 Windows 及 Linux 主機架設安全防護 」
 - ✓ 「 個資法與我的關係暨個資案例宣導分析 」



第一場-eduroam無線漫遊建置

□ 111年3月22日 (二)

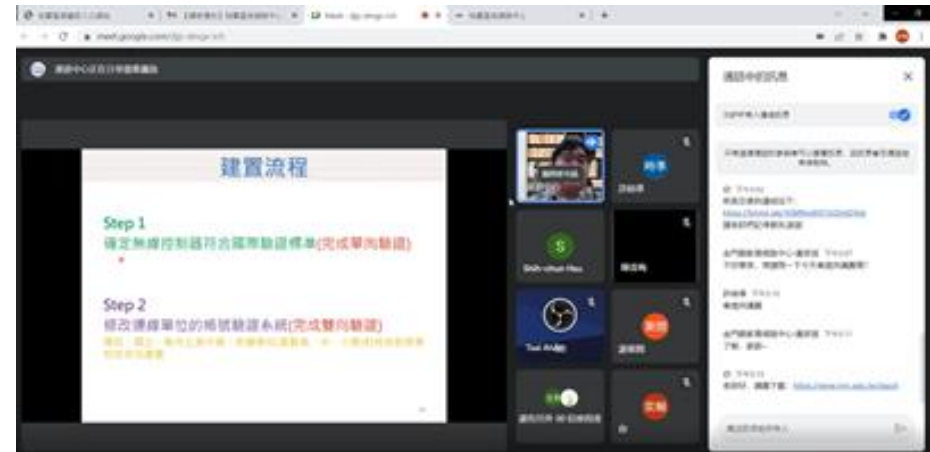
□ eduroam無線漫遊建置

□ 講師：張家倫先生/
東華大學臺灣學術無線網路漫遊中心

□ 上課人數：49人(疫情影響，採線上視訊)

□ 課程大綱

1. 加入漫遊建置
2. 架設認證伺服器
3. 設定無線控制器
4. 確定內部架構和帳號驗證系統
5. 模組設定與測試



第二場-IT工作壓力的調適與舒壓

□ 111年05月04日（三）

□ IT工作壓力的調適與舒壓

□ 講師：蔣懷孝老師/中原大學

□ 上課人數：42人(採線上視訊)

□ 課程大綱

1. 從心理與運動談壓力
2. 從健康的人生談壓力
3. 運動、疲勞與睡眠
4. 運用心理學與行為歸因
5. 溝通的問題
6. 七何分析法
7. Q&A



第三場-資安線上講座「資通安全概論」

□ 111年06月15日（三）

□ 資安線上講座「資通安全概論」

□ 講師：劉得民老師/

中華民國網路封包分析協會理事長

□ 上課人數：102人(採線上視訊)

□ 課程大綱

第1單元 資通安全基本觀念

第2單元 電子郵件社交工程與防範

第3單元 認識加密勒索與預防

第4單元 資料防護與備份

第5單元 個資蒐集、管理與保護

第6單元 密碼設定與存取原則

第7單元 個人電腦安全性設定

國際資安現況趨勢

網路資安攻擊的主要項目

- 94%的惡意程式採用電子郵件方式傳送。
- 用戶端電腦的已知資安事件，超過 80% 的入侵方式，為網路釣魚攻擊。
- 主機端電腦的資安(外洩)事件，60%為漏掉修補程式沒有安裝更新。
- 40% 的 網路資安主管認為，網路安全欠缺足夠人力。

用戶端電腦設備
社交工程的誘惑，魚叉式、水坑式攻擊，仍然是主要手法，只是，附件檔案多半為 Office檔案、PDF檔案、RAR/ZIP、ISO 檔案。

智慧型手機與平板設備
透過手機與平板設備的URL下載APK方式，與無厘手機內建惡意程式，成為注目焦點!!

IoT 網路設備
除了 IoT設備的CVE漏洞之外，又加入社群媒體網路內建密碼曝光，導致大範圍 IoT 設備被攻擊。

第四場-資安其實很簡單

□ 111年08月26日（五）

□ 資安其實很簡單

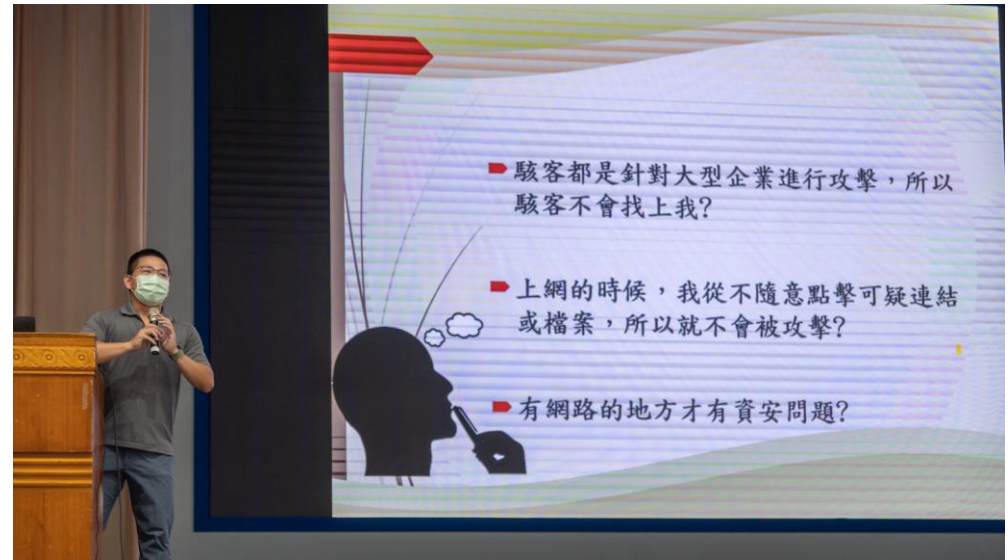
□ 講師：張二川技正/

國立中央大學電子計算機中心

□ 上課人數：150人

□ 課程大綱

1. 桃園區網簡介
2. Public IP 、 Private IP 、 NAT
3. 無孔不入的社交工程
4. 勒索病毒與惡意程式
5. 資料備份321
6. IOT設備防護



第五場-勒索軟體與防治資料外洩應對指引

□ 111年09月07日（三）

□ 勒索軟體與防治資料外洩應對指引

□ 講師：蔡一郎執行長／

微智安聯股份有限公司 創辦人暨執行長

□ 上課人數：125人(採線上視訊)

□ 課程大綱

1. 全球資安威脅與攻擊事件分析
2. 勒索軟體成為主要的威脅
3. 如何建立數位韌性



第六場-校園資安防護及資安法因應

□ 111年09月21日（三）

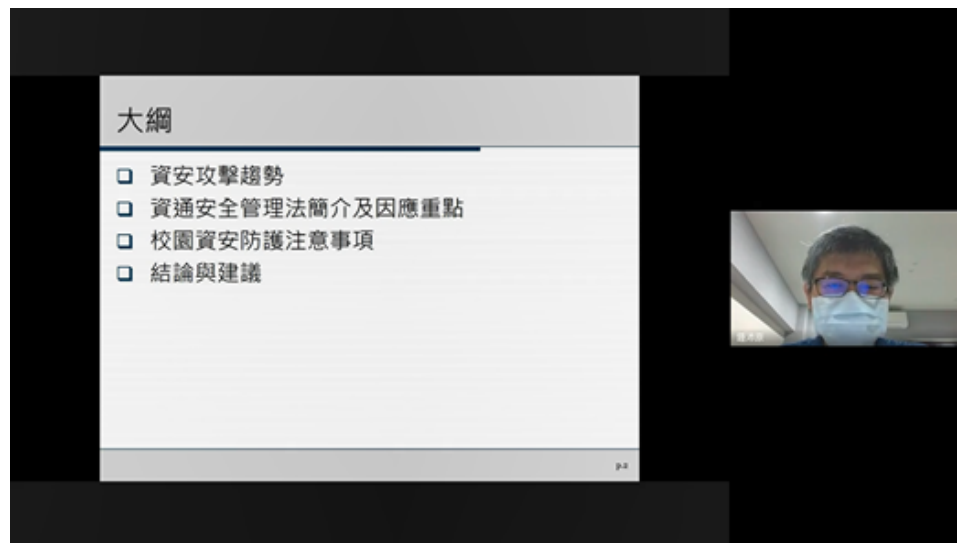
□ 校園資安防護及資安法因應

□ 講師：鍾沛原專案經理/
國立成功大學資通安全研究與教學中心

□ 上課人數：116人(採線上視訊)

□ 課程大綱

1. 資安攻擊趨勢
2. 資通安全管理法簡介及因應重點
3. 校園資安防護注意事項
4. 結論與建議



第七場-主機滲透測試與 vulnhub 靶機初探

■ 111年10月13日（四）

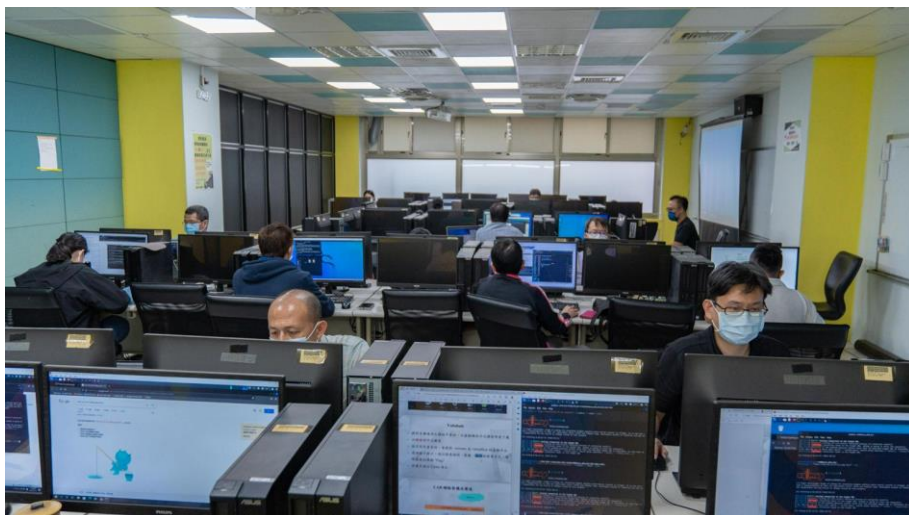
■ 主機滲透測試與 vulnhub 靶機初探

■ 講師：施衣喬老師/
國立宜蘭大學圖書資訊館

■ 上課人數：27人

■ 課程大綱

- (1) vulnhub 平台介紹
- (2) 檢測工具使用及介紹
- (3) 套件網站弱點與因應對策
- (4) 主機權限弱點與因應對策
- (5) Q&A



預計年底前教育訓練

- 第八場：11月30日 資安入侵事件的調查與應變
- 講師：陳昱崇 處長/
詮睿科技股份有限公司
- 課程大綱：藍隊角度探討入侵事件處理常見問題 or 按照原本的 資安入侵事件的調查與應變。
 1. 事件處理經常遇到的困擾
 2. 常被攻擊者利用的對象
 3. 主動出擊的小撇步
 4. 事前、事中與事後
 5. 真實 APT 案例分享 (KMP SCA、Operation DRBControl)
 6. 最新攻擊趨勢的演進
 7. 常用事件調查工具介紹
 8. 常見網站攻擊案例分享
 9. 來個實際發生的情境題



重大營運事件之檢討



- 本年度桃園區網中心無重大營運(網管及資安)事件。

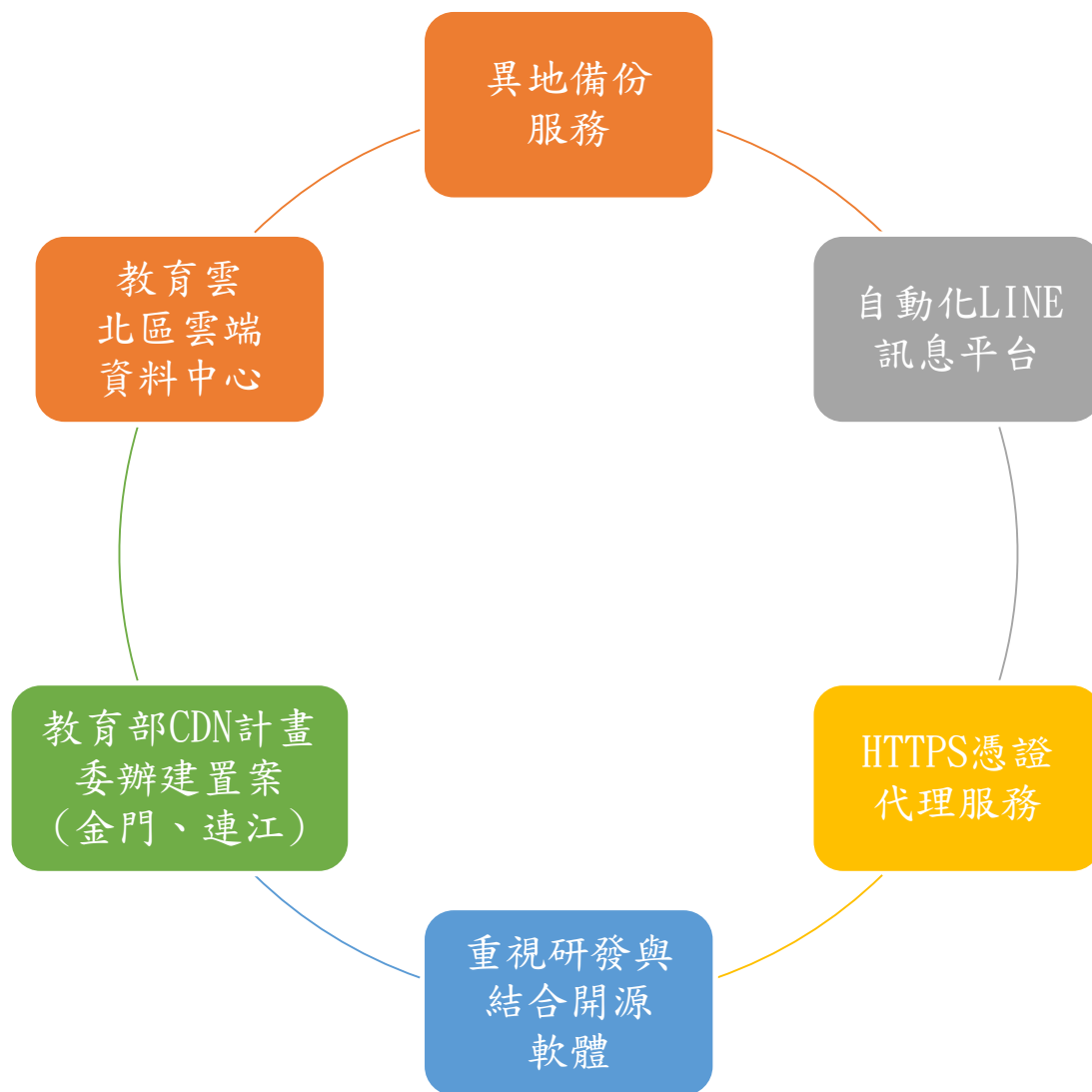


第四章



特色服務

特色服務



異地備份服務(1)

- ❑ 異地備份是推動資訊安全管理的重要工作之一，以面對災難後，可以復原重要資料讓業務持續運行，然而進行異地備份租賃機房費用昂貴。
- ❑ 花蓮區網(國立東華大學)與桃園區網(國立中央大學)於111年9月19日簽署合作備忘錄，雙方平等互惠使用對方儲存空間為異地備份。
- ❑ 協助雙方連線學校避免因勒索病毒、地震、火災等不預期意外，造成學校重要資料損失。

The screenshot displays a Zoom meeting interface. On the left, a Microsoft Word document is open, showing the title '國立東華大學與國立中央大學「資料異地備份」合作備忘錄' (Memorandum of Understanding for Data Off-site Backup between National Dong Hwa University and National Central University). The document content includes the purpose and content of the agreement, mentioning the use of each other's storage space for off-site backup. On the right, a grid of participants is visible, including Yi-Ming Chen, 志偉, 陳偉銘, 志偉, 桃園區網中心_柯..., 李宇峰, 東華大學_何振揚, and 你. The meeting title at the top of the Zoom window is '國立東華大學與國立中央大學「資料異地備份」合作備忘錄'.

異地備份服務 (2)

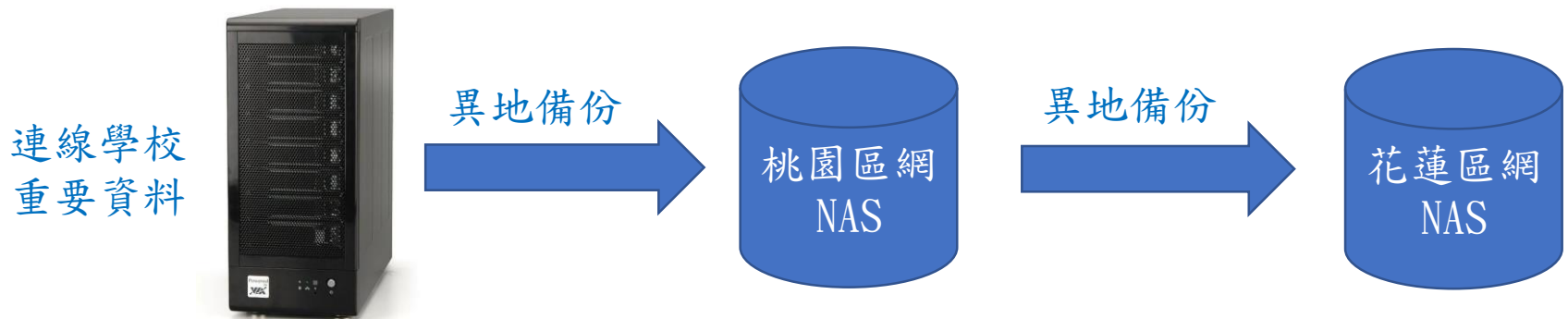
❑ 為確保重要資料之機密性，雙方請轄下連線單位各自事先加密以確保資料之隱密性。

❑ 異地備份空間額度

✓ 高中職：1TB（未來將提升至2TB）

✓ 大專院校：2TB

✓ 縣市教育網路中心：4TB



異地備份服務 (3)

- ❑ 連線單位向桃園區網中心申請異地備份時，可選**是否**將備份資料再往花蓮區網備份。
- ❑ 第一次完整備份後，隨後進行差異備份，可節省頻寬
- ❑ 每三日備份一次，保留版本數:5
- ❑ 桃園區網及花蓮區網雙方初期先提供20T空間



直線距離超過100公里

異地備份服務(4)

序	項目	說明
1	系統功能	異地備份，提供區網連線學校申請使用。
2	地理位置距離	100公里以上
3	防護縱深	IPS、核心路由器ACL、防火牆
4	機房ISMS 制度	通過第三方驗證
5	異地資料備份方式	完整備份與差異備份、資料備份五代
6	實體環境保護	電力、空調、門禁、監視、消防環境符合ISMS規定
7	網路配置	目前異地備份網路頻寬1G，11月底即將提升至10G

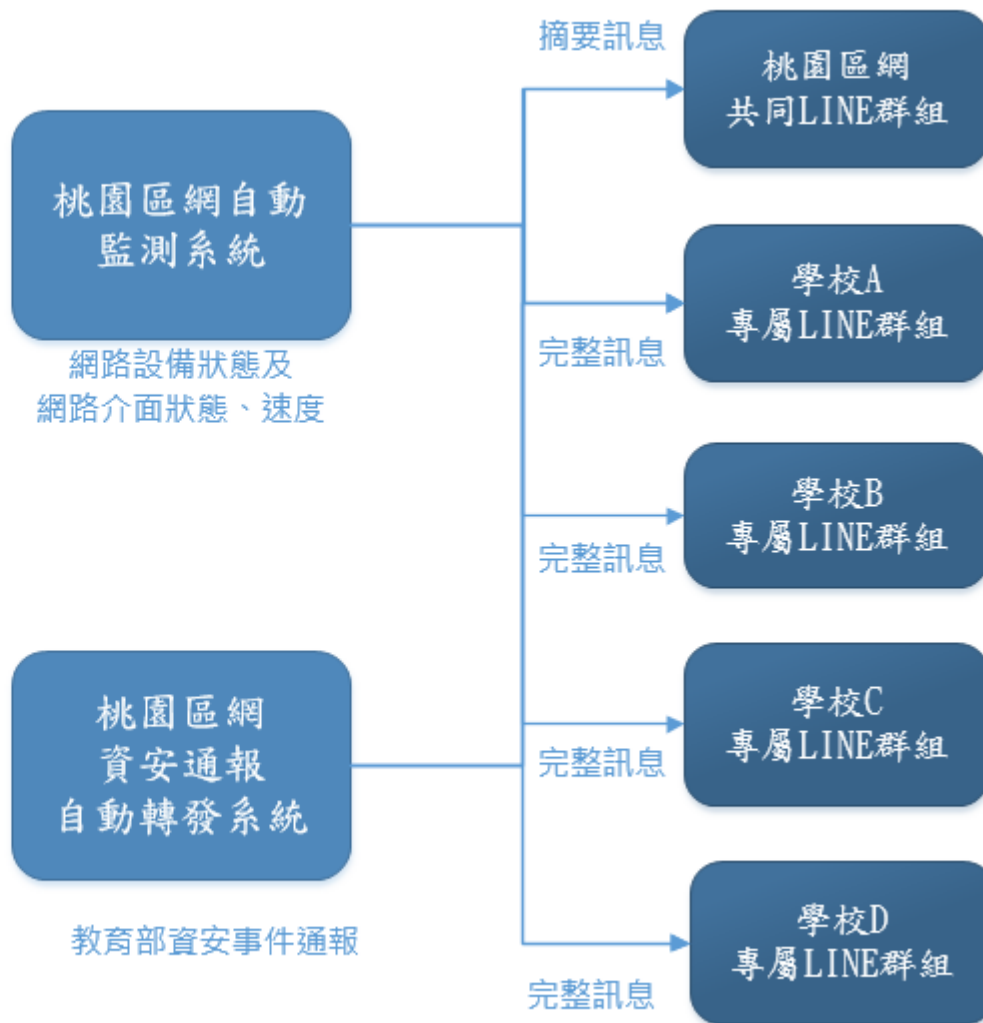
連線學校異地備份建置進度

□ 目前已協助6所高中職、2所大學、1所縣市網路中心完成異地備份至桃園區網中心，並以自動排程備份到100公里外的花蓮區網中心。

序	異地備份申請學校	完成日期
1	振聲高中	111/08
2	六和高中	111/08
3	治平高中	111/10
4	長庚大學	111/10
5	大興高中	111/10
6	新興高中	111/10
7	啟英高中	111/10
8	連江縣網	111/10
9	萬能科大	111/10

區網自動化LINE訊息平台(1)

桃園區網自動化 LINE訊息平台

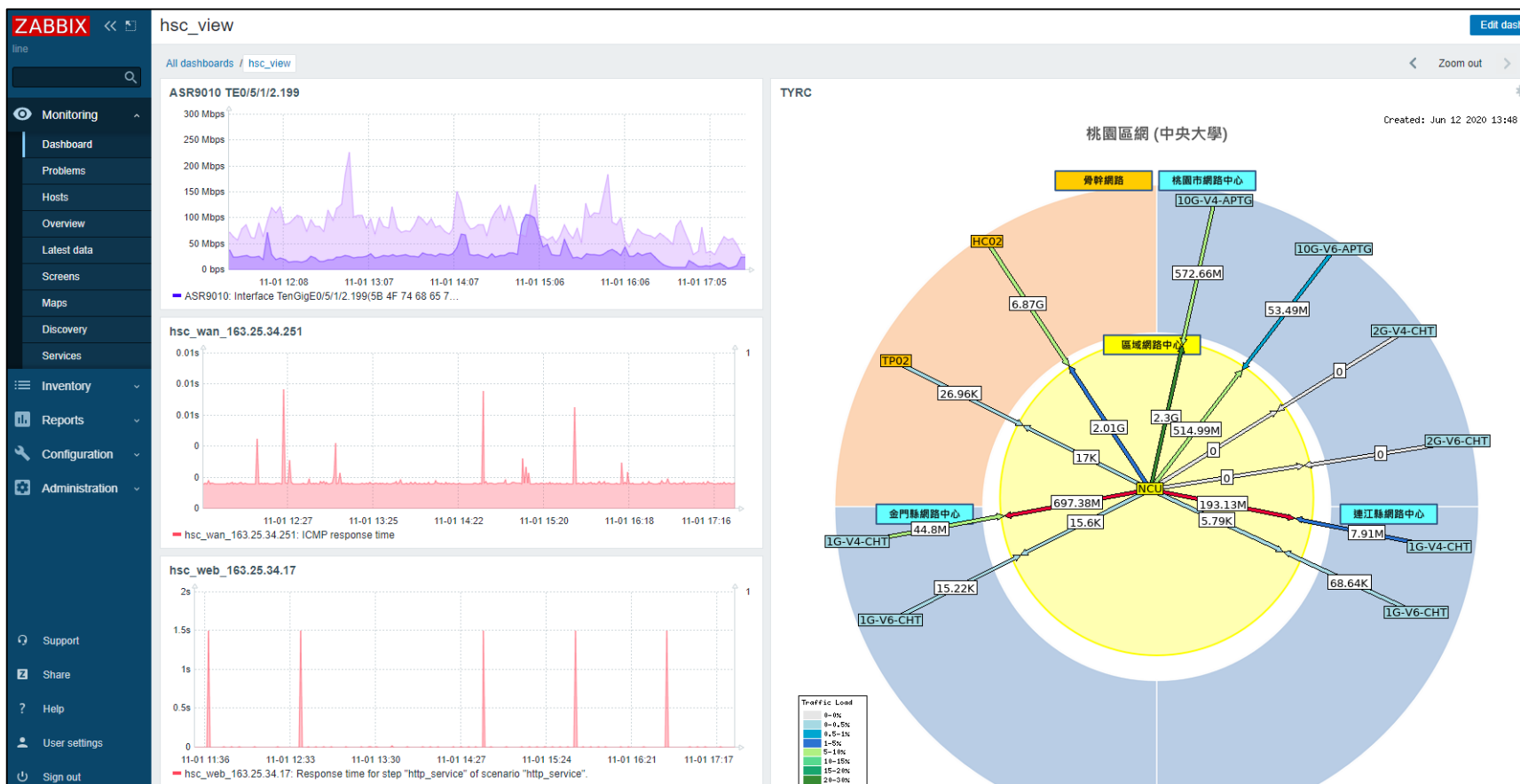


自動化LINE訊息平台(2)



自動化LINE訊息平台(3)

1. 監測區網ASR9010核心路由器對學校的網路介面流量
2. 監測連線學校的對外WAN IP 狀態
3. 監測連線學校的網站服務是否正常



自動化LINE訊息平台(4)

監測網路設備狀態及
介面狀態及速度，以
LINE即時告警



當收到LINE訊息告警
，請檢視貴校網路對
外是否正常？

桃園區網、振聲高中合作群
組 (4)



LINE Notify

4月25日(一)

【TYRC_Notify】
[TYRC-5596235] 問題已解
決: Unavailable by ICMP
ping

主機: fxsh_wan

問題解決時間: 06:15:37 on
2022.04.25

Problem duration: 1m

【TYRC_Notify】
[TYRC-5596237] 發生問題:
High ICMP ping loss

主機: fxsh_wan

狀態: Loss: 66.67 %

時間: 06:15:37 on
2022.04.25

Severity: Warning

上午 6:15

桃園區網&萬能科技大學合
作群組 (7)



LINE Notify

10月24日(一)

【tyrc_notify】[NEW]-教育機構
資安通報-(萬能科技大學
120.124.34.112)資安預警情
報(發布編號:NISAC-
EWA-202210-23898)

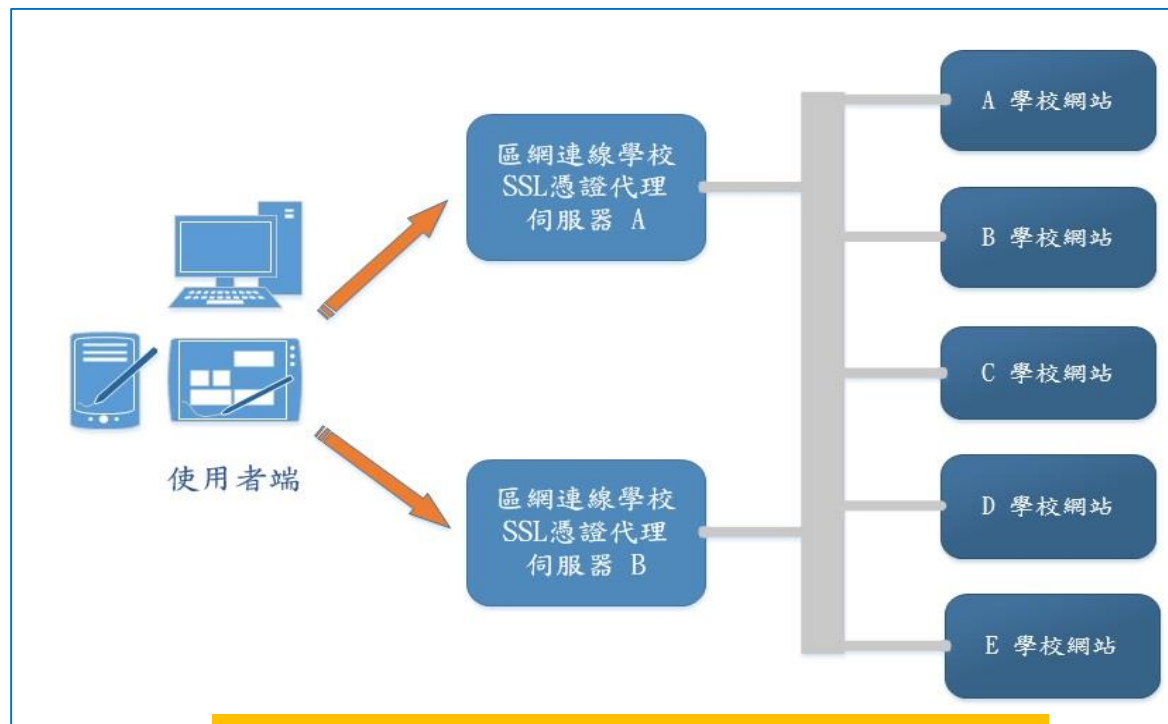
下午 6:48

自動化LINE訊息平台(5)

序	加入LINE訊息平台 學校	完成日期
1	振聲高中	111/03
2	北科附工	111/03
3	永平工商	111/03
4	新生醫專	111/04
5	金門縣網中心	111/05
6	桃園市網中心	111/05
7	六和高中	111/05
8	萬能科大	111/10

HTTPS 憑證代理服務(1)

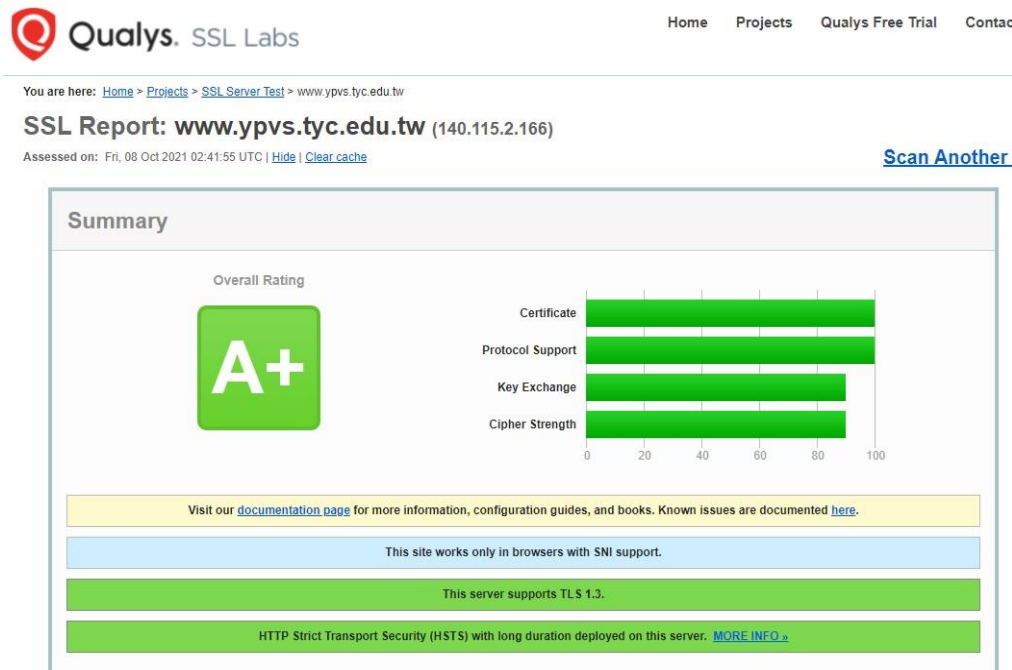
- 教育部110年6月29日臺灣學術網路(TANet)技術小組第96次會議決議，各級學校網站應導入 HTTPS。
- 桃園區網中心利用開源軟體NGINX的反向代理特性，達成後端網站伺服器的SSL憑證代理，110~111年累計完成8所學校，共16個學校網站導入HTTPS。



論文發表於TANET2021研討會

HTTPS 憑證代理服務(2)

- ❑ 26% 的學校網站不需要更動原網站設定及網站程式碼，順利導入HTTPS。
- ❑ 74% 的學校網站也能在區網協助下共同檢視，修改網站設定及調整網站程式以導入HTTPS，完成導入HTTPS。
- ❑ 憑證代理使用TLSv1.2，TLSv1.3，以及HSTS (HTTP Strict Transport Security)，協助連線學校網站取得A+ 安全性評等。



HTTPS 憑證代理服務(3)

序	學校	HTTPS 憑證代理 完成日期
1	大華高中 thsh	110/08/11
2	振聲高中 fxsh	110/08/19
3	永平工商 ypvs	110/08/30
4	啟英高中 cyvs	110/09/01
5	成功工商 ckvs	110/09/24
6	復旦高中 fdhs	110/10/05
7	大興高中 dxhs	110/10/14
8	育達高中 yuda	111/01/24

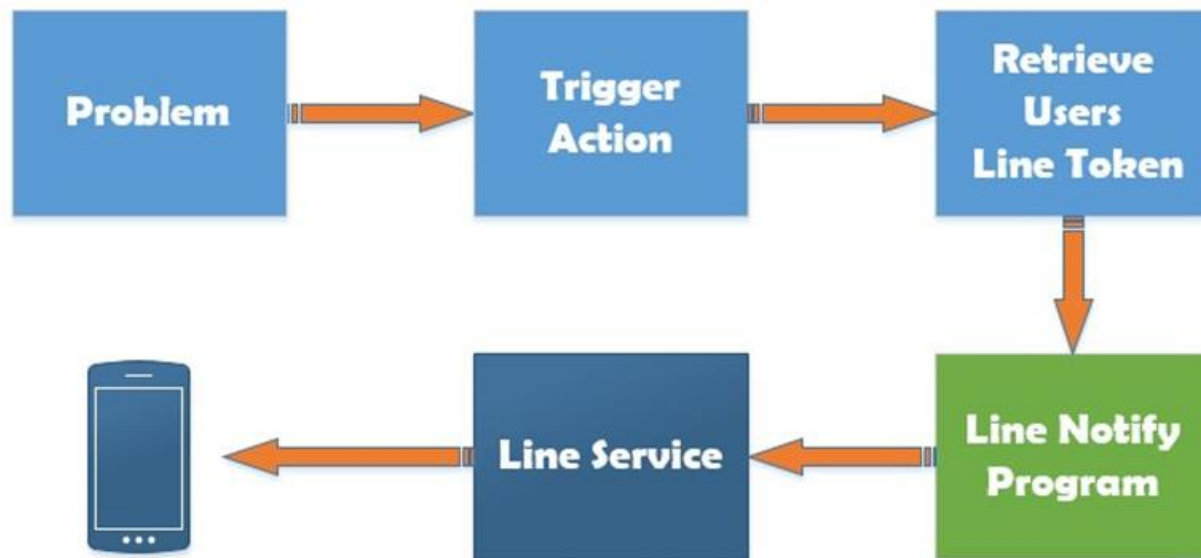
重視研發與結合開源軟體(1)

□ 桃園區網面對網路管理以及資安的各项需求，試著以開源軟體為基礎，並結合自行開發的程式以完成各項任務，並將這些經驗投稿至TANET研討會。

研討會名稱	論文題目	備註
TANET2021研討會	SSL憑證代理伺服器之建立與導入-以桃園區網中心為例	
TANET2020研討會	自動監測系統結合LINE 即時訊息通知-以桃園區網中心為例	最佳人氣論文獎
TANET2019研討會	Open Source Security Onion 系統之導入與應用-以桃園區網中心為例	
TANET2018研討會	Open Source SIEM系統之導入與應用 -以桃園區網中心為例	佳作論文獎
TANET2017研討會	以網路分流器彈性部署入侵偵測與防禦系統-以桃園區網中心為例	
TANET2016研討會	自動化調整雲端Spark異常流量偵測系統	
TANET2015研討會	結合 Spark 與 Hadoop於雲端平台進行網路異常流量偵測	

重視研發與結合開源軟體(2)

- ❑ 2020年桃園區網中心透過導入開源Zabbix系統，監測重要網路設備、機房溫溼度，以確保網路及機房設備全年無休的正常運作。
- ❑ 區網中心並自行開發LINE Notify程式，即時發送LINE Notify訊息，讓網管人員隨時掌控機房環境及網路服務是否正常運作。

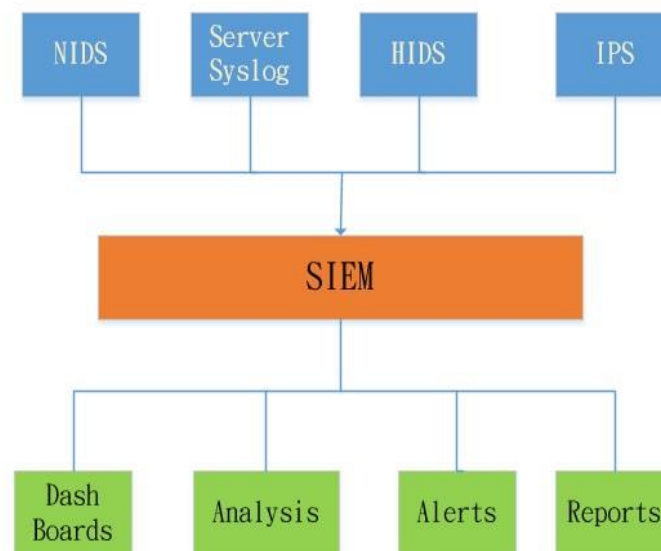


TANET2020研討會最佳人氣論文獎

重視研發與結合開源軟體(3)

□ 2018年桃園區網中心透過導入開源OSSIM系統，即時監控網路行為並且針對HIDS、NIDS及IPS等系統事件收集、管理及分析。

□ 藉由SIEM系統的視覺化儀表板、警示訊息、報表等功能，提供關連的資安事件，找出網路環境中的威脅。



TANET2018研討會佳作論文獎

重視研發與結合開源軟體(4)

- 2015年自行開發Spark異常流量偵測系統，系統由Spark模組負責即時的運算，可以充分利用 Spark in-memory computing特性，在大量的NetFlow Data中快速找出異常網路行為的主機。
- Hadoop模組則處理大量批次作業，以每小時進行大量資料分析作業。



TANet桃園區網Spark+Hadoop流量監測

[\[連線學校 MRTG流量\]](#) [\[IPv6 MRTG流量\]](#) [\[Links 連線狀態偵測\]](#) [\[設備工具庫\]](#) [\[回報主機檔\]](#)

NCU (回報主機檔系統)

TopN 流量

- TopN 流量排行
- TopN 流量 (小時)

UDP Flooding 流量監看

- UDP Flooding 流量

UDP 詳細流量

- UDP 流量排行
- Udp 流量 (小時)
- Udp 流量 (10分鐘)

Pecan 異常

- Pscan 異常流量排行
- Pscan 異常流量 (小時)
- Pscan 異常流量 (10分鐘)

TopP 封包量

- TopP 封包量排行
- TopP 封包量 (小時)
- TopP 封包量 (10分鐘)

UDP Flooding 偵測 (Kscore)

Keyword:

Hostip	輸入量(MB)	輸出量	輸入連接數	輸出連接數	輸入封包大小	輸出封包大小	輸入封包量	輸出封包量	紀錄時間
140.138.83.253@1	23	2503	175	770	201	1133	115392	2207872	10-20 10:00
142.251.42.238@1	3176	1113	6251	7306	1112	714	2854976	1559104	10-20 10:00
142.251.43.14@17	595	1839	7080	7459	544	930	1093504	1977408	10-20 10:00
142.251.43.16@17	78	8099	40	51	86	1369	901824	5916160	10-20 10:00
142.251.43.1@17	60	3690	2168	3156	112	1306	538304	2824256	10-20 10:00
163.25.123.26@17	9	1030	58	42	116	1367	80576	753408	10-20 10:00
163.25.27.65@17	0	1296	16	34	119	1119	1216	1158144	10-20 10:00
163.28.51.12@17	315	39331	6360	7406	80	1354	3906880	29027840	10-20 10:00
163.28.51.13@17	294	37950	6340	7369	79	1358	3703488	27940608	10-20 10:00
163.28.51.14@17	302	35095	5749	6640	79	1363	3820160	25730240	10-20 10:00
163.30.106.91@17	714	1263	1071	942	1049	1190	681472	1061568	10-20 10:00
172.217.160.110@	260	1012	4578	5546	426	864	610944	1170560	10-20 10:00
172.217.160.65@1	20	1535	488	694	81	1342	256704	1143360	10-20 10:00

教育部CDN委辦建置案

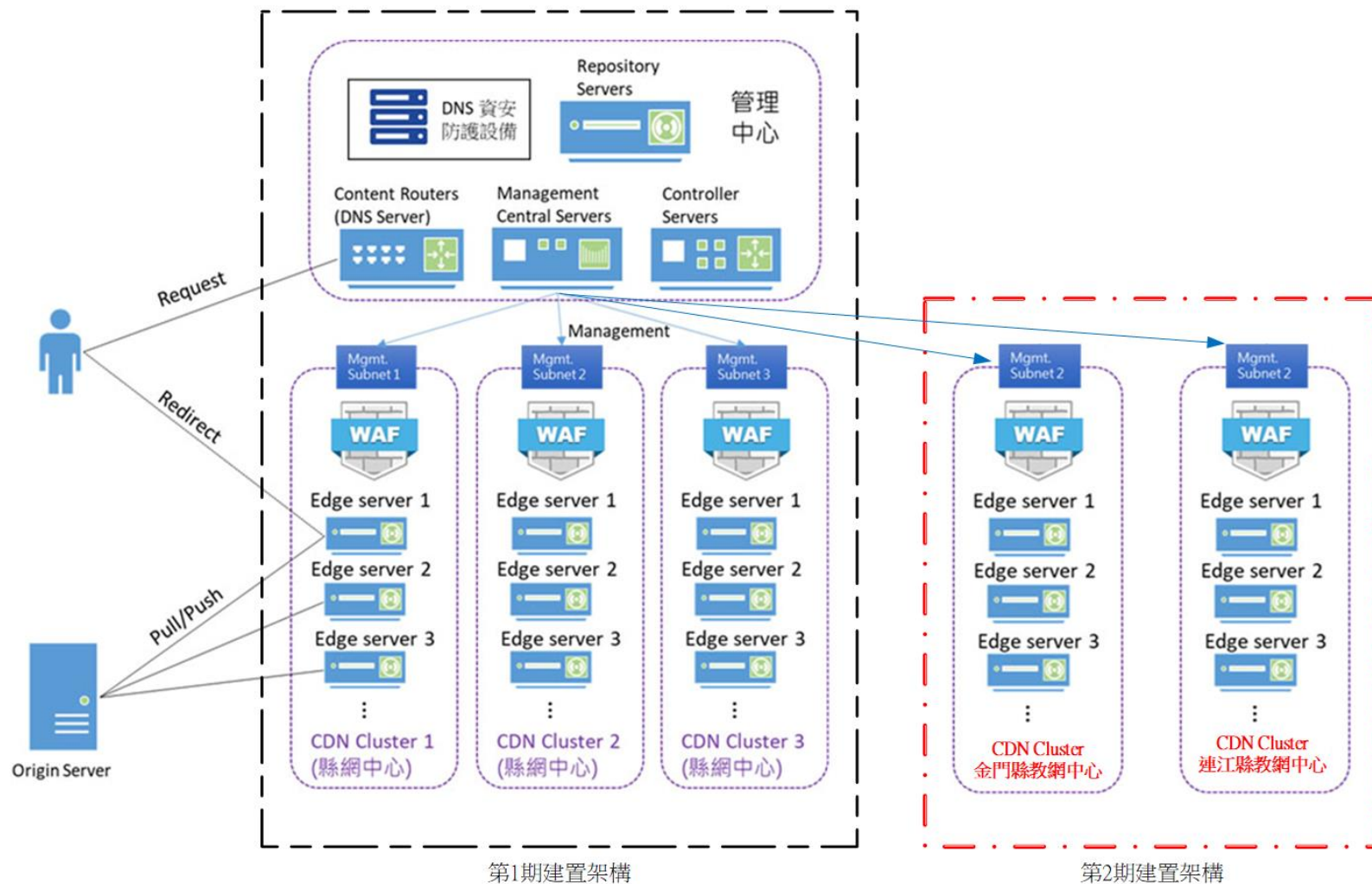
□ 教育部111年7月8日臺教資(四)字第1112702634A號函委託桃園區網辦理「臺灣學術網路(TANet)內容傳遞網路建置計畫-第2期」建置案。

- 期程：至111年12月31日，必要時得展延至112年3月31日
- 建置單位：金門縣及連江縣教育網路中心

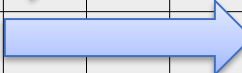
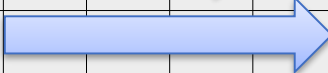
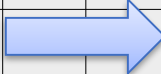
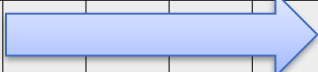
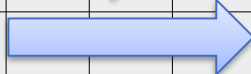
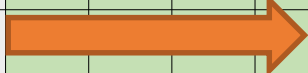
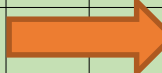
□ 金門縣及連江縣分別建置：

- 硬體規劃為伺服器 4 台、WAF 2 台、48 埠交換器 2 台。
- Edge、WAF 為高可用性設計，避免單點失效之情形發生。
- 整體架構與教育部第1期已建置之 CDN 服務整合。

教育部CDN委辦建置案-整合架構圖



教育部CDN委辦建置案-期程及規劃

	2022年										2023年				
	3	4	5	6	7	8	9	10	11	12	1	2	3	4	
承接金門縣、連江縣網CDN建置案															
洽詢本校資訊往來廠商															
撰寫計畫書報部及修訂															
架構確認及調整															
計畫正式核定 確認及撰寫採購規格書															
進行請購作業及正式上網公告															
金門縣及連江縣CDN建置施工															
整合測試															
驗收及結案															
整備期											建置期				

提供的資源

- CPU: 216 vCPU (108 core)
- RAM: 1504 GB
- HD: 可用 70TB (鏡像的備份)

使用的軟體

- 雲端管理軟體
 - VMware
- 虛擬化儲存軟體



教育雲上的服務系統詳細資源

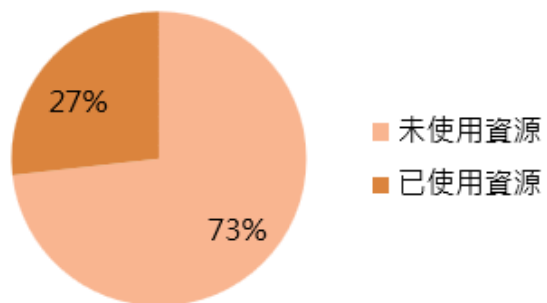
111年持續穩定提供雲端資料中心服務，截至目前共有14項服務系統，承載了69台虛擬機，使用資源總計vCPU 406、vRAM 972 GB、vHD 49.19 TB

服務系統名稱	vm數量	vCPU	vRAM	vHD
TANet_VoIP	3	12	48	240
中華開放教育平台	11	48	152	24519
字音字形網	1	8	16	160
英語線上學習平台	2	48	128	3050
教育單位弱點檢測平台	1	8	16	100
教育媒體影音	6	24	48	11165
教育體系單一帳號驗證授權平臺	10	80	208	950
教師研習平台	4	32	64	3589
微積分題庫	1	4	8	100
數學小學堂系統	3	14	28	1301
體育署_體育雲-全民運動資訊系統	13	60	120	3956
體育署_體育雲-全民運動資訊系統報名網站	9	40	80	900
體育署_體育資訊雲端	3	12	24	300
磨課師	2	16	32	40
總計	69	406	972(GB)	49.19(TB)

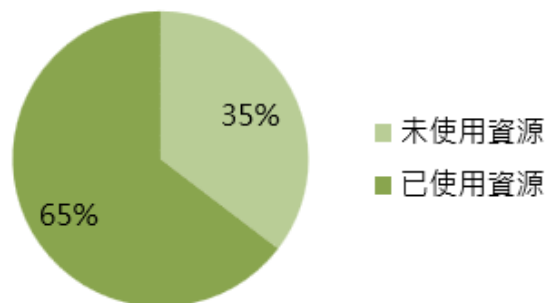
教育雲北區雲端資料中心—資源使用情況

項目	*vCPU	vRAM (GB)	vHD(TB)
總資源量	216	1504	70
未使用資源	158.13	532.00	20.81
已使用量	57.87	972.00	49.19
已使用量(%)	26.79%	64.63%	70.27%

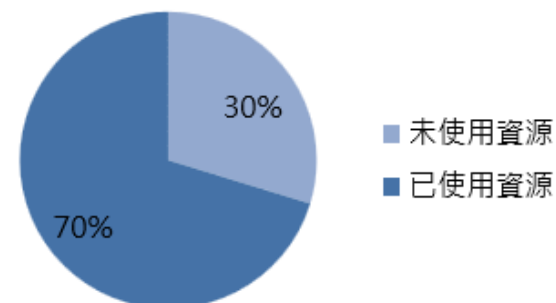
vCPU



vRAM



vHD



教育雲北區雲端資料中心-績效服務

教育雲服務為教育部管制，本中心負責營運，111年度教育雲無重大事件發生，持續提供穩定服務。



CPU使用率



RAM使用率

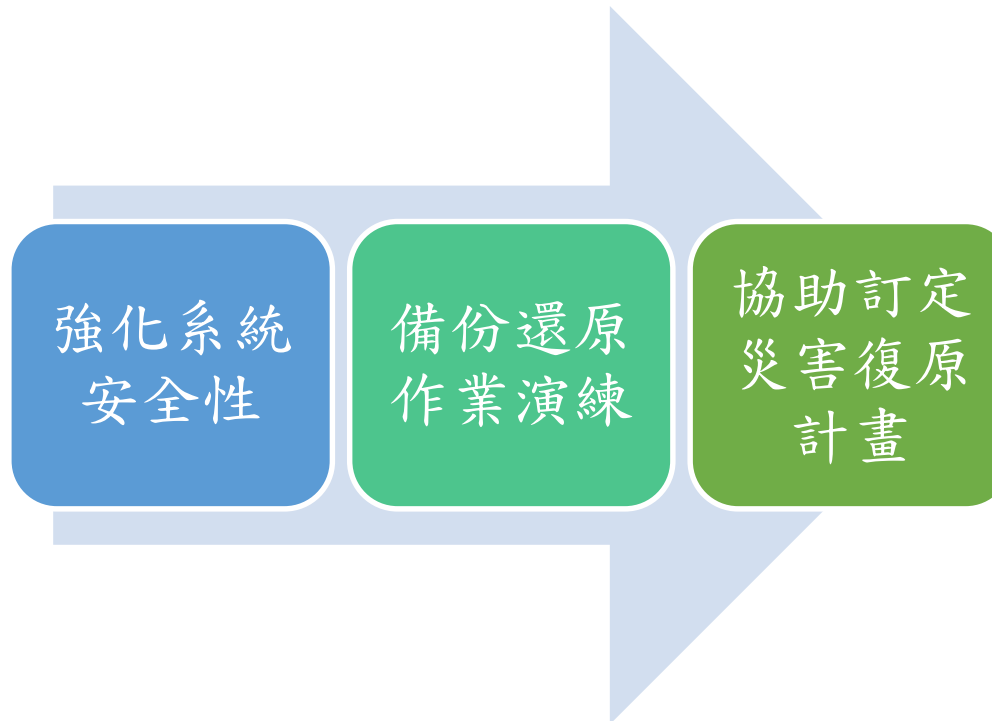


未來營運方針與 創新服務 目標

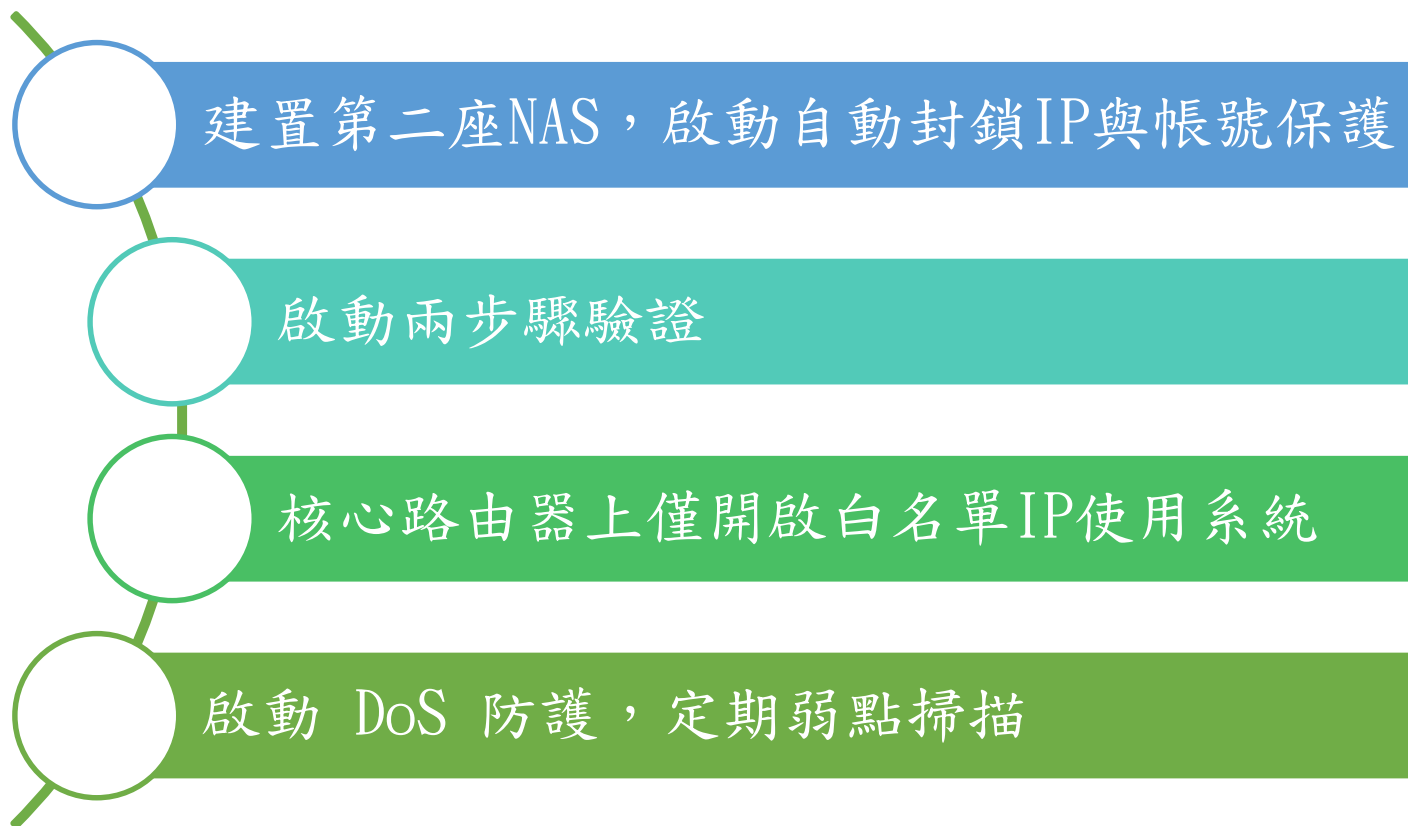
未來營運方針

項次	112年度 KPI指標	目標值
1	全年電路服務妥善率	99.99%
2	召開區域網路中心管理會議，邀請連線單位分享該校網路管理經驗。	召開2次會議，出席率90%
3	辦理網路管理及資訊安全教育訓練，課程實質效益分析，50%以上課程需進行前測與後測。	辦理 7 場。後測進步平均達 20%以上。
4	協助連線學校進行弱點掃描、網站網頁檢測等資安服務	7所學校
5	連線學校之IPv4/IPv6推動完成率。	90%
6	提供離島縣市教育網路中心網路管理、資安研習、巡檢網路機房環境或技術支援服務。	1次
7	提供連線學校資安巡迴服務	3次
8	異地備份服務使用率	40%連線學校

強化異地備份服務



強化系統安全性



備份還原作業演練

定期測試異地備份資料，
確保其可用性。

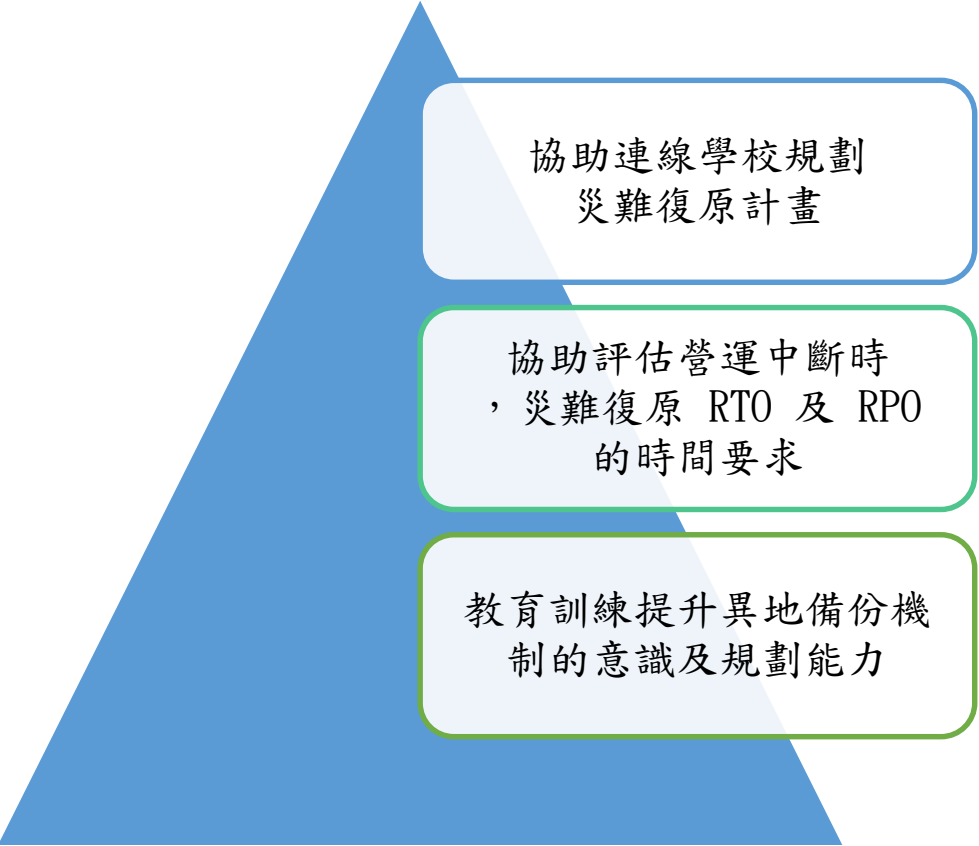


定期檢查測試回復程序。



定期協助連線學校演練，
使用異地備份資料還原。

協助連線學校訂定災難復原計畫

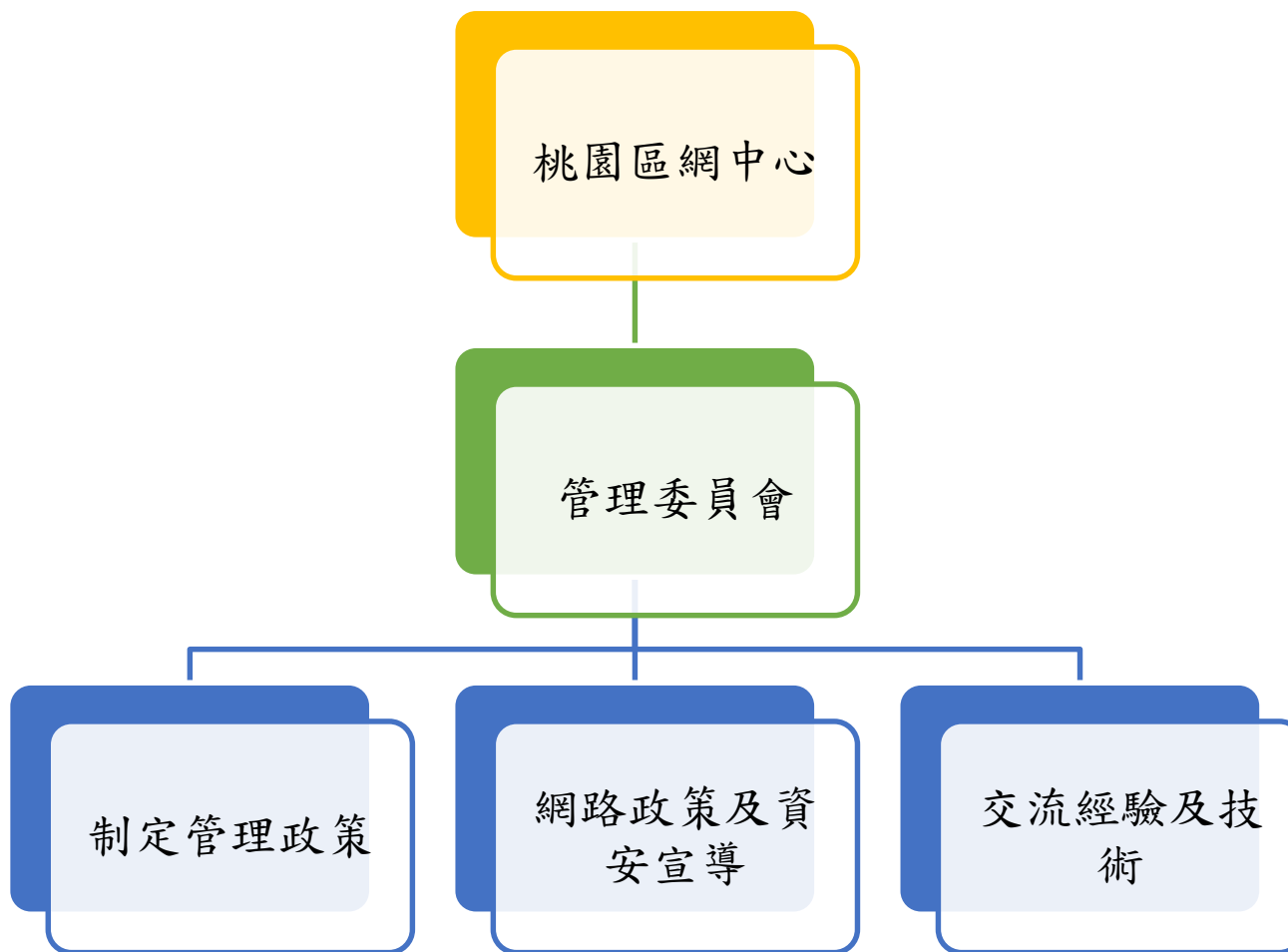


協助連線學校規劃
災難復原計畫

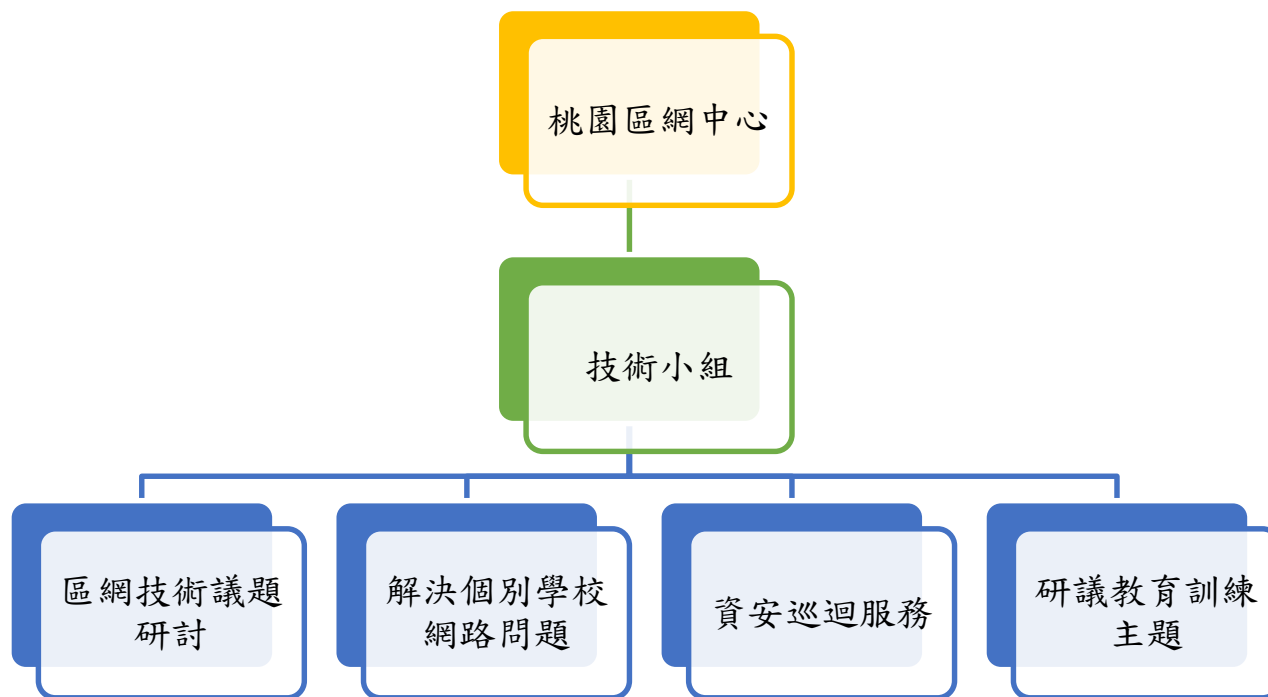
協助評估營運中斷時
，災難復原 RTO 及 RPO
的時間要求

教育訓練提升異地備份機
制的意識及規劃能力

成立桃園區網技術小組(1)



成立桃園區網技術小組(2)



- ❑ 邀請有熱忱的連線學校夥伴，結合他們的技術與經驗，成立技術小組。
- ❑ 技術小組將共同研討區網技術議題、解決學校網路問題、資安巡迴服務、研議教育訓練主題。



第五章



成效精進

執行成效精進情形(1)

項次	110年度委員建議	改進及精進做法
1	弱掃復掃改善程度可以強化量化數據	今年復掃加強追蹤高風險及中風險處理情形，並提供相關修補量化數據。
2	書面基礎資料提供建議可強化當年度績效及下年度目標，事件的說明宜有更清楚。	遵照委員指示辦理，加強書面基礎資料當年度績效說明及下年度目標，並清楚說明當年度完成工作。
3	區網中心維運包含教育雲端服務，宜有更清楚的雲端維運績效說明。	由於教育雲服務均由教育部提供，亦由教育部進行資源設定，本中心則持續提供穩定的雲端資料中心服務，截至目前共有14項服務系統，承載了69台虛擬機。
4	教育訓練課程建議可將內容加以數位化，並妥適公開給連線單位學習，並建立循環改善機制。	今年完成7門課程影片上架於Moodle線上學習系統 https://eustoma.cc.ncu.edu.tw/ ，並導入前後測機制，後測分數比前測分數進步20%。

執行成效精進情形(2)

項次	110年度委員建議	改進及精進做法
5	下年度的目標宜有更明確的質化和量化的指標，將更能突顯自我精進的特色。	遵照委員指示辦理，已加強下年度目標明確的質化和量化的指標。
6	以積極協助連線學校導入 IPv6 網路環境，已有初步成效，但建議在明年度完成所有學校之相關設定，若有問題可了解反應之。	遵照委員指示辦理，已完成85%的學校導入IPv6，另外15%的部分包含路由器設備不支援的3所學校，及遺失路由器帳號密碼的2所學校。預計明年協助遺失路由器帳號密碼的2所學校重設密碼後建置，屆時可達90%。
7	以完成 11 所高中職 DNS 向上集中，建議明年度可完成 100%連線單位DNS 版本更新。	遵照委員指示辦理，對於不熟悉bind編譯升級，或擔心影響正在上線DNS服務的連線學校，由桃園區網中心遠端連線三所大專院校編譯安裝最新之bind版本，預計年底可順利達成100%更新。

執行成效精進情形(3)

項次	110年度委員建議	改進及精進做法
8	桃園區網協助連線學校導入 HTTPS 過程中，大專院校有比高中職較多的人力與資源，而公立國高中學校有市網中心協助，但私立高中職學校網站升級 HTTPS 是否可思考區網提供網站代管服務來解決此問題。建議可思考如何協助轄下各級機關學校符合資通安全管理法相關要求，若有相關問題可考慮那些問題區網可協助解決，那些要反映給教育部處理。	1. 提供高中職網站代管服務，必須提供足夠的虛擬機資源，並強化網站的資安才能達成網站代管，受限資源不足，暫未提供網站代管服務。 2. 本年度提供連線學校異地備份服務，協助連線學校避免因勒索病毒、地震、火災等不預期意外，造成學校重要資料損失。 3 提供資安巡迴服務，協助連線學校檢視資安防護能力及檢視網路架構。

111年KPI指標執行率

項次	111年度 KPI指標說明	執行情形
1	全年電路服務妥善率：99.9 %以上。	本年度無斷線紀錄
2	召開 2 次區域網路中心管理會議，邀請4個連線單位分享該校網路管理經驗。	100%
3	辦理 6 場網路管理及資訊安全教育訓練，課程實質效益分析，50%以上課程需進行前測與後測，前測與後測分數進步平均達 20%以上。	100%（今年辦理7場次，67%以上課程進行前測與後測，後測分數比前測分數進步20%）
4	協助至少 7 所連線學校進行弱點掃描、網站網頁檢測等資安服務。	100%（今年協助8所學校弱點掃描472個主機，檢測54個網站）
5	100% 大專院校導入 IPv6 ，85% 高中職連線學校導入 IPv6（目前有 2 所私立高中職回報該校路由設備並不支援 IPv6）。。	大專院校已達100%，今年完成6所高中，但有3所高中路由設備不支援IPv6，另有2所遺失路由器密碼，整體IPv6建置率 85%。
6	每年至一個離島縣市教育網路中心提供網管資安研習、巡檢網路機房環境或技術支援服務。	100%（計畫12月8日赴馬祖）

綜合建議

- ❑ 校園網路出口頻寬不足，ISP業者線路租賃費用造成負擔
- ❑ 協助區網學校向中華電信談談tanet 頻寬能否原價升速。



2022

桃園區網中心

許時準組長

center20@cc.ncu.edu.tw