南投區域網路中心
110年度年終審查

國立暨南國際大學/計算機與網路中心

報告人：陳彥良、劉育瑄

基礎維運資料-年度經費

本年度經費使用情形：

教育部核定計畫金額：160 萬元

教育部補助計畫金額： 160 萬元

區網中心自籌金額： 3 萬1080元 (租用發電機)

實際累計執行數（1月-11月）：約150萬元 ，執行率93%。

基礎維運資料-中心人力配置

專任：18人　　兼任：2人

其中包含教育部補助：無補助雲端管理人員

1. **網路管理 1人 證照數4張**
   - ISO 27001 資訊安全管理系統、BS 10012個人資料管理系統、網路架設丙級、職能評量證書-資通系統風險管理
2. **資安管理 1人 證照數7張**
   - ITE 網際網路介接基礎、ITE 資料通訊、ITE 網路安全、ITE 網際網路服務與應用、網路架設乙級技術士技、CHFI 資安鑑識調查專家認證、職能評量證書-網路架設與部署安全

基礎維運資料-年度經費

歷年經費使用情形：

年度	核定補助經費	年度達成率	備註
107	1,390,000	100%	經費無須繳回
108	1,395,000	99.95%	經費無須繳回
109	1,400,000	100%	經費無須繳回
110	1,600,000	93%	計算至11月

基礎維運資料-人力

人員任務配置：

在職年度	職稱	姓名	人員配置
98年-迄今	網管人員	劉育瑄	骨幹網路監測及故障排除 資安事件之通報、應變、審核及事件資料收集與分析 計畫經費控管及計畫行政業務 ISMS 系統導入及驗證、資通安全法導入 區網網頁管理 配合教育部進行資安通報演練、社交工程演練 舉辦教育訓練及IPv6推廣相關活動 協助連線單位弱點掃描 提供連線單位各事項反應及聯絡窗口及其他交辦事項
103年-迄今	資安人員	陳彥良	骨幹網路監測及故障排除 資安事件之通報、應變、審核及事件資料收集與分析 防火牆管理，阻擋 DDoS 攻擊，降低 DDoS 對網路服務的影響 配合教育部進行資安通報演練、社交工程演練 協助弱點掃描、連線單位資訊安全健診 機房環境監測及電力設備維護 提供連線單位技術協助及其他交辦事項

基礎維運資料-人力

人事經費運作情形：

年度	核定人事費	人事費餘額	備註
107	1,294,387	452	流用至業務費 經費無須繳回
108	1,316,208	694	經費無須繳回
109	1,328,605	0	經費無須繳回
110	1,333,152	0	經費無須繳回

基礎維運資料-網路及資安管理

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
下游連線學校或連線單位數統計	連線學校(單位)數	1	2	10	1	9	連線單位總數 23
	連線單位比例	4.35%	8.70%	43.48%	4.35%	39.13%	註：單位數 / 總數

基礎維運資料-網路及資安管理

區域網路中心連線資訊彙整表：

連線頻寬與電路數統計	專線(非光纖)						
	光纖	10M(不含)以下		1			1
		10M(含)以上100M(不含)以下					1	1
		100M(含)以上 500M(不含)以下			12	1	8	21
		1G(含)以上 10G(不含)以下	4					4
		10G(含)以上		2				2
	其他(如ADSL等)							
	連線電路小計		4	3	12	1	9	29
	連線頻寬合計 (電路實際租用頻寬加總)		4096m	20485m	1200m	100m	820m	連線頻寬總計： 26701m
	連線頻寬比率		15.34%	76.72%	4.49%	0.37%	3.07%	請加總電路實際租用頻寬/總計頻寬

基礎維運資料-網路及資安管理

區域網路中心連線資訊彙整表：

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.	南投縣教育網路中心	連線頻寬(1)	中華電信1G×2	4G
			連線頻寬(2)	亞太電信1G×2	
非學校之連線單位(不含ISP)	連線單位名稱		連線頻寬		備註
	1.	台大清水溝	100M		
	2.	台大溪頭	100M		
	3.	台大下坪植物園	100M		
	4.	台大水里	100M		
	5.	台大內茅埔	100M		
	6.	台大和社	100M		
	7.	台大水里營林區	100M		
	8.	台大竹山	20M		
	9.	台大對高岳營林區	100M		

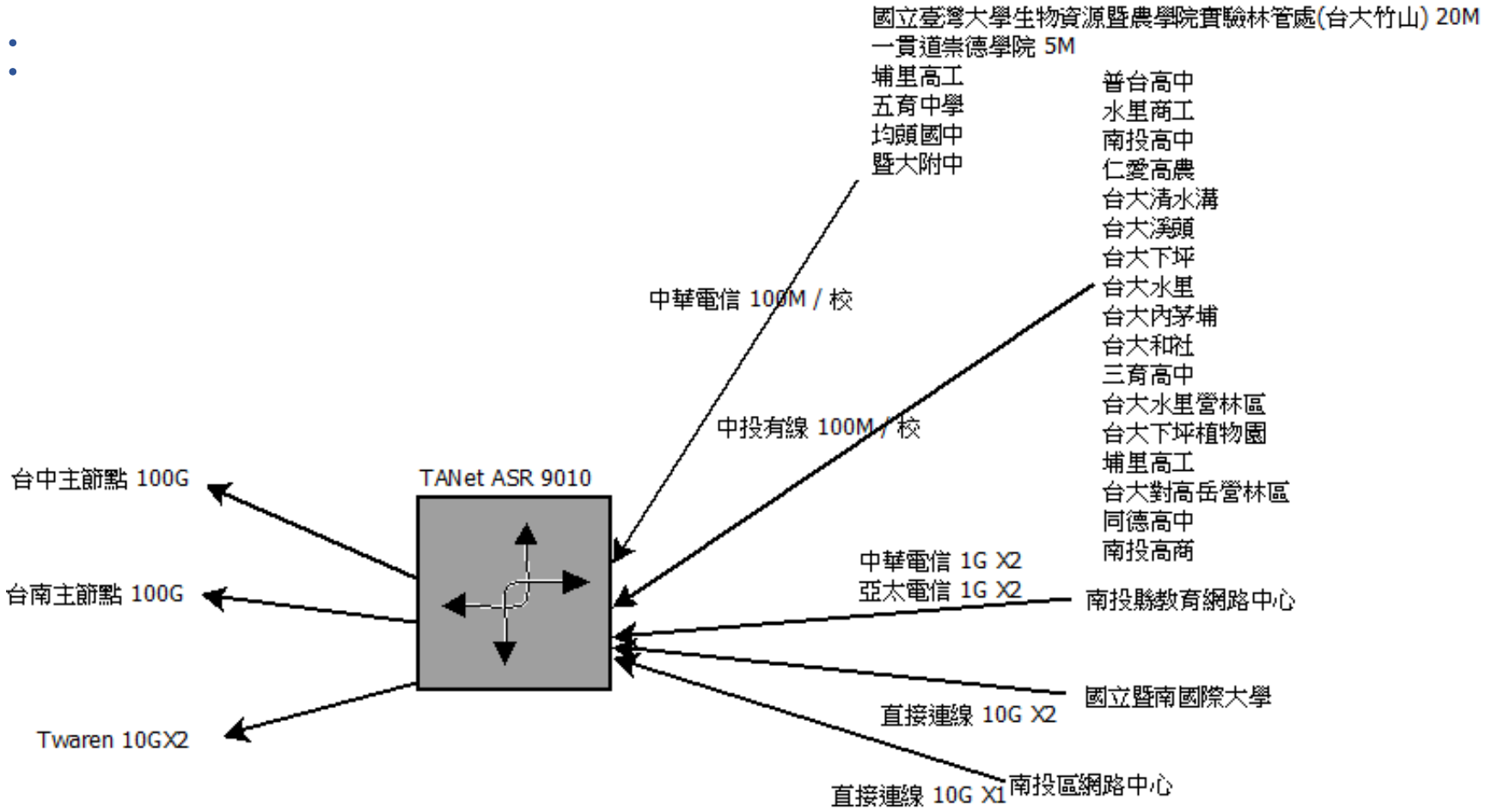
基礎維運資料-網路及資安管理

區域網路中心連線資訊彙整表：

		主節點名稱	連線頻寬	備註
連線TANet	1.	台中主節點	100G	
	2.	台南主節點	100G	

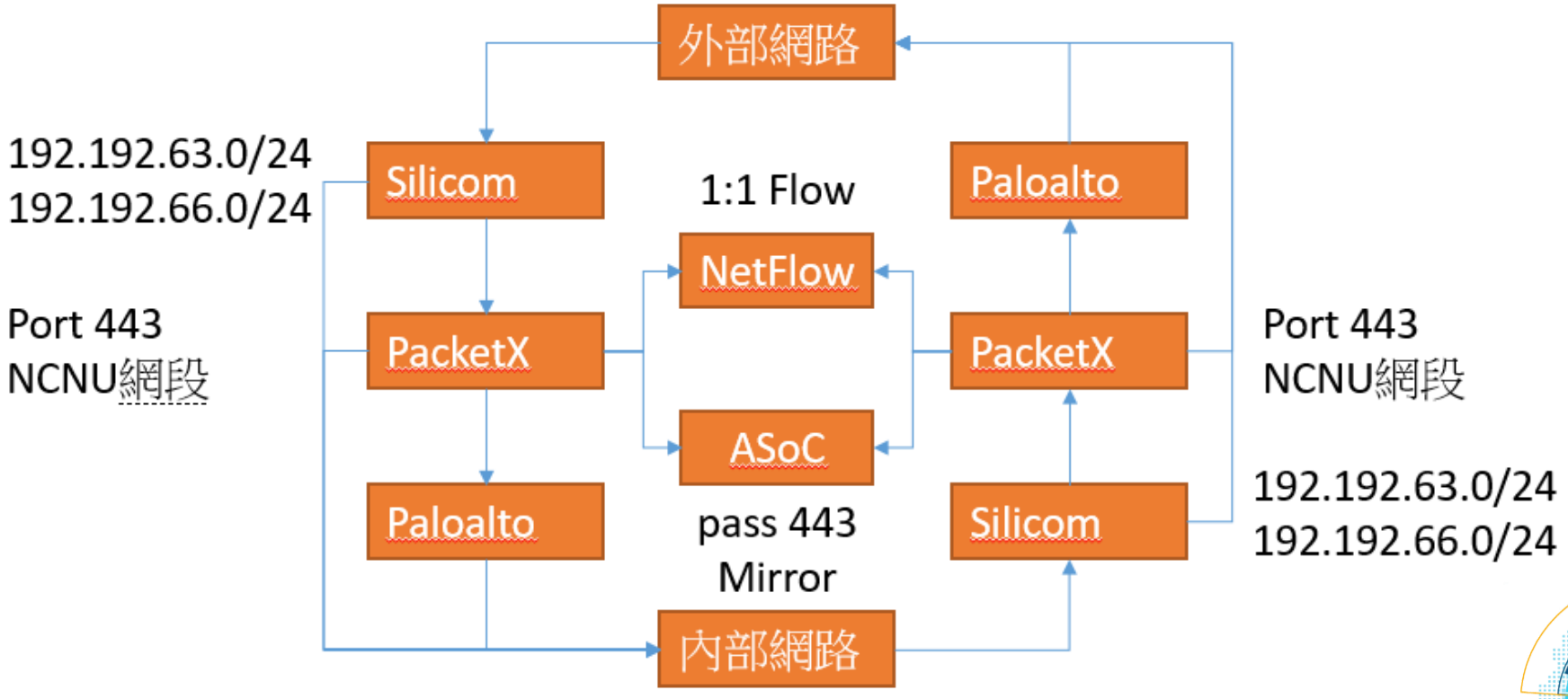
基礎維運資料-網路及資安管理

網路架構圖：



基礎維運資料-網路及資安管理

網路資安架構圖：



基礎維運資料-網路及資安管理

區域網路中心資訊安全環境整備表：

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

1、2級資安事件處理：

1) 通報平均時數：0.06小時
2) 應變處理平均時數：0.21小時
3) 事件處理平均時數：0.75小時
4) 通報完成率：100%
5) 事件完成率：100%

資安事件通報審核平均時數：
0.05小時。

本年度並無3、4級資安事件

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：100%

基礎維運資料-網路及資安管理

區域網路中心配合本部資安政策：

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 100 %

本中心符合

✓資安專業證照人數達8人（ ISO27001 主導稽核員證照）

✓維護之主要網站進行安全弱點檢測比率：100%

區網網站定期進行弱點掃描並進行修補

具體辦理事項-網路管理

110年度網路管理維運具體辦理事項：

✓持續提供NetFlow查詢系統並開放給連線單位使用

N-Reporter 收集1:1 NetFlow 資訊，可提供精確且詳細資料供連線單位自行查詢，並有統計各單位流量排名等功能，當流量雍塞時找出異常使用 IP。

✓提供 cacti 可回溯的流量紀錄與查詢

可查詢各連線單位每日、每星期、每月、每年等區間的統計流量，網頁連結 https://www.ntrc.edu.tw/cacti/traffic3.html。

具體辦理事項-網路管理

110年度網路管理維運具體辦理事項：

✓What's Up 監測:

監測骨幹與連外反應狀態，包含骨幹路由器 ASR9101、骨幹防火牆 Paloalto5060、骨幹分流設備 PacketX、機房 UPS，另外針對網路有偵測台中主節點、台南主節點、與各連線單位節點狀態，可提供可用率 (Availability) 、回應時間 (Response Time) 與斷線告警。

✓分流設備:目前有三個主要作用

- 過濾加密流量進入資安設備降低資安設備負擔。
- 產生 1:1 NetFlow。
- 將流量拆解分別送入兩台 ASOC 所架設的 FirePower 中做異常行為偵測。

具體辦理事項-網路管理

110年度網路管理維運具體辦理事項：

✓提高 IPv6 設定率:

推動 IPv6 Dual-Stack 環境，南投區網共有 14 間連線單位（不包含台大實驗林分部），至今年 4 月已完成 14 間連線單位實地網路環境訪視及現況訪談，區網端 IPv6 設定率已達100%，有 11 間完成 Web Server IPv6 設定及 Web Server 支援 IPv6 正解，5 間完成網頁取樣分析設定。

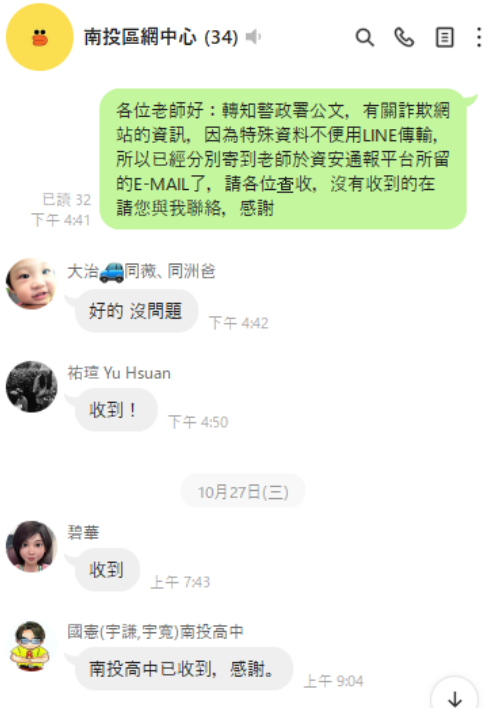
具體辦理事項-網路管理

110年度網路管理維運具體辦理事項：

✓召開連線單位管理委員會，已於本年10/12日召開第一次線上管理委員會，預計於12月召開第二次管理委員會

✓建置連線單位LINE群組，提供便捷快速的分享及交流空間。

✓協助新成立的唯心聖教學院進行連線介接相關事宜。



具體辦理事項-網路管理

110年度網路管理維運具體辦理事項：

✓機房環控監測：

- 門禁：本中心依 ISMS 規定進行機房門禁管制。
- 溫濕度：本中心依 ISMS 規定機房溫濕度，機房溫濕度異常時將會發出簡訊及電子郵件告知。
- 漏液偵測：機房內設有漏液偵測設備，當漏水時可以第一時間發簡訊告警通知維運人員。
- UPS 不斷電系統：機房 UPS 緊急供電能力達 1.5 小時，並一季做一次基礎保養及放電測試。
- 市電及發電機保養：每年 7 月進行重電保養確保電力系統穩定供電，另設有電力監測系統，當發生市電中斷會第一時間發簡訊告警。

具體辦理事項-網路管理

110年度網路管理維運具體辦理事項：

✓機房環控監測：

- 機房消防：於骨幹區與 UPS 室設有獨立偵煙設備，當發生火災時會以簡訊通知維運人員。
- 極早期火災預警系統是一種靈敏度非常高的的空氣取樣式煙霧偵測系統。它的偵測方式是藉由主機內部的抽氣泵，透過分佈四處的取樣管路將防護區域內的空氣樣品抽回主機內部進行分析比對，當空氣中的煙霧濃度到達一定程度時，系統就會即時發出預警。若能在火災醞釀初期及時產生預警訊號，就能提供更多的時間來抑制火災的生成與發展，以防止重要的資產與設備非預期的重大損失。

- 參考資料：https://fps.secom.com.tw/product.asp?page=&forid=31&ext=43

具體辦理事項-網路管理

110年度網路管理維運具體辦理事項：

✓極早期火災預警系統

具體辦理事項-網路管理

110年度網路管理維運具體辦理事項：

✓極早期火災預警系統

抽風管

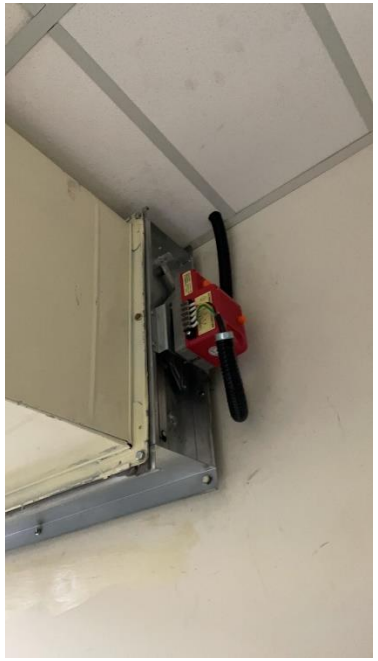
主機

具體辦理事項-網路管理

110年度網路管理維運具體辦理事項：

✓機房環控監測：極早期火災預警系統

- 可燃物、溫度(燃點) 、助燃物(氧氣)
- 外氣引入系統 – 提供新鮮的氧氣
  - 當火災發生實需警急停止外氣引入系統 運作



電動風門

外氣引入
控制箱

具體辦理事項-網路管理

110年度網路管理維運具體辦理事項：

✓機房環控監測：極早期火災預警系統

極早期火災預警系統		
極早期偵測系統	**環境監測系統**	**外氣引入系統**
➢ 主動偵測空氣中煙霧濃度 ➢ 觸發火警訊號 ➢ 發出警報(聲光)	➢ 接收火警訊號 ➢ 發送簡訊 ➢ 觸發外氣警急停止	➢ 戶外溫度低於 20度引入外氣 ➢ 上班時間停止運作 ➢ 警急停止開關

具體辦理事項-網路管理

110年度網路管理維運具體辦理事項：

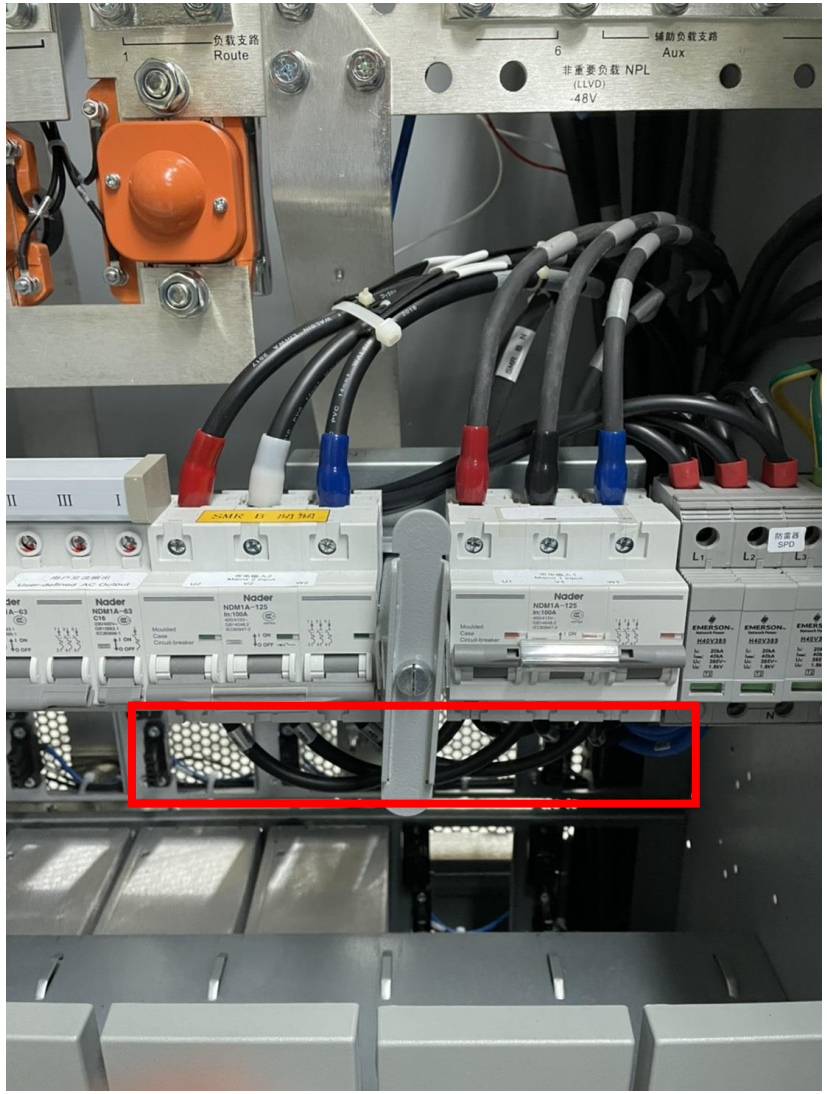
✓機房環控監測：

- 第二迴路發電機：因應圖資大樓重電保養時無法啟用大樓緊急發電機與近年來保養時間越來越長，於今年完成第二路緊急電力施工，可於圖資大樓重電保養時另外租用發電機供電。
- 於今年 7/11 重電年度維護保養作業使用。
- 第二迴路發電機僅供給 SMR 與機房空調使用

具體辦理事項-網路管理

110年度網路管理維運具體辦理事項：

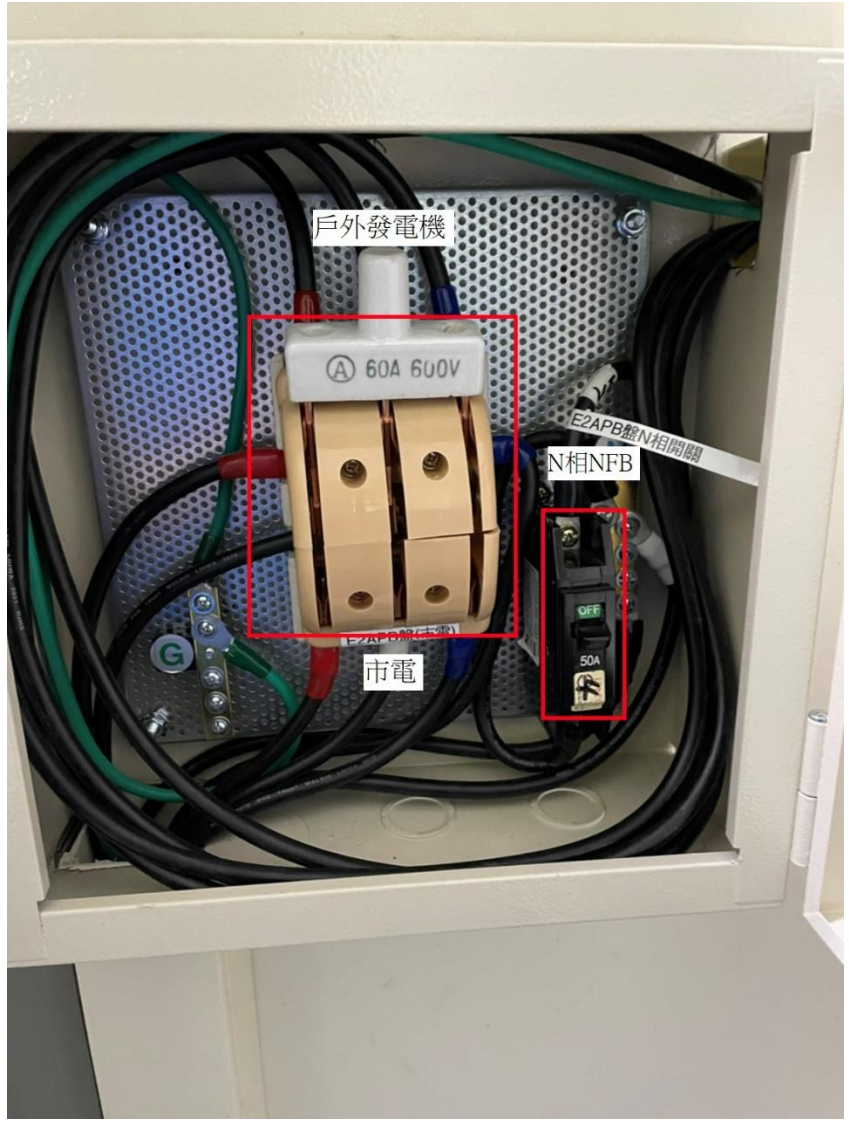
- 第二迴路發電機：兩迴路不可同時開啟，不然會有短路風險，每次操作都需要先將兩個開關切到 OFF，在將需要的迴路送電，確保安全。



具體辦理事項-網路管理

110年度網路管理維運具體辦理事項：

- 第二迴路發電機：空調使用雙投閘刀開關，須無負載情況下切換，有負載的情況下可能無法切離，有負載的情況下投入會產身火花，操作時會由空調的控制面板關閉電源後再做切換動作。



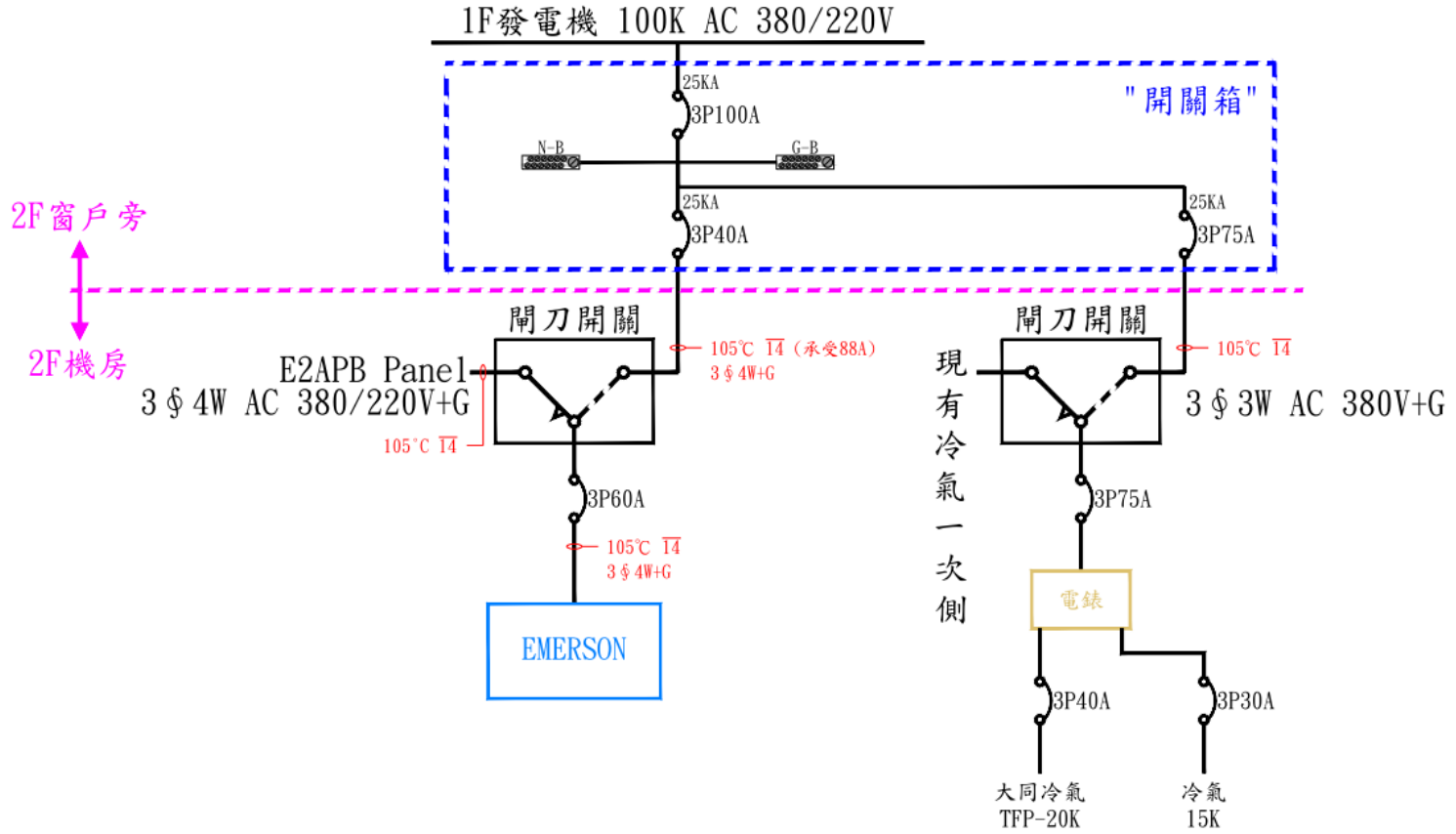
具體辦理事項-網路管理

110年度網路管理維運具體辦理事項：

- 第二迴路發電機-配電箱：

具體辦理事項-網路管理

- 第二迴路發電機-配電圖：



具體辦理事項-網路管理

第二迴路發電機：電力操作有人身安全風險，設計操作查核表

- 相序是否正確
- 相序錯誤冷氣無法運作，安裝發電機時確認即可
- 電壓是否正確
- 發電機啟動後須確認電壓是否正確，過高電壓會燒毀設備，過低的電壓設備無法啟動
- SMR 內開關不可同時切到 ON
- 空調切換前需要先關閉空調開關再切換

具體辦理事項-網路管理

111年度網路管理營運方針：

(一)　持續監控及機房管理

(二)　持續提供 NetFlow 查詢系統。

(三)　持續提供 cacti 可回溯的流量紀錄與查詢。

(四)　至少召開 2 次管理委員會。

(五)　確保電力備援及發電機、UPS 等保養維護。

具體辦理事項-資安服務

110年度資安服務維運具體辦理事項：

✓參與北區 ASOC 中心計畫區網建置兩台 FirePower 入侵防禦系統，並透過 TACERT 台灣學術網路危機處理中心平台派發資通安全事件。

✓骨幹防火牆，主要進行流量過濾與惡意清單封鎖，並針對基本 DoS 攻擊進行阻擋達到第一道防線的功能。

✓網頁弱點掃描，本中心每年幫連線單位進行兩次網頁弱掃服務，本年度許多連線單位為配合政策將網頁進行向上集中，故協助連線單位修改網頁後再次弱掃服務。

具體辦理事項-資安服務

110年度資安服務維運具體辦理事項：

✓協助台大實驗林進行資安健診惡意網域與 IP 偵測

- 使用技服名單為測試基準
- 技服名單內有惡意 IP & DN
- 透過 mirror port 產生 NetFlow 收集 IP 資訊
- 透過 mirror port 擷取封包，側錄用戶端詢問 DNS 資訊

具體辦理事項-資安服務

110年度資安服務維運具體辦理事項：

✓協助台大實驗林進行資安健診惡意網域與 IP 偵測

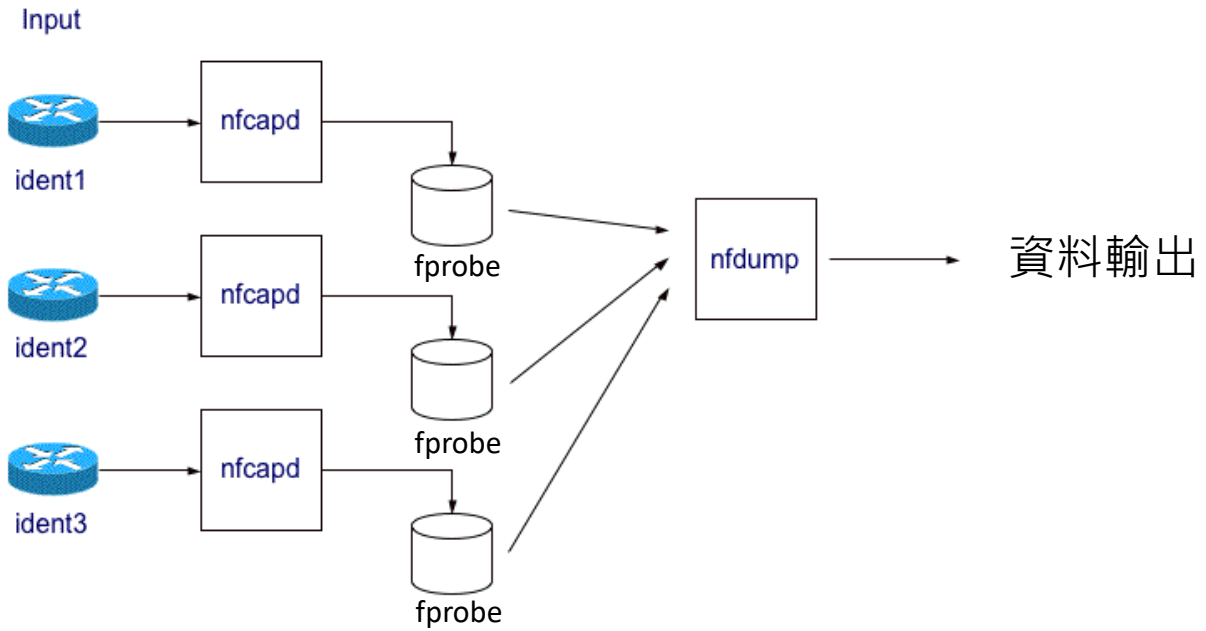
- NetFlow
  - Nfcapd –產生 NetFlow 資料
  - fprobe – 儲存 NetFlow 資料
  - Nfdump – 比對 NetFlow 資料
- 擷取封包
  - tcpdump – 擷取封包
  - tashark – 資料比對

具體辦理事項-資安服務

110年度資安服務維運具體辦理事項：

✓協助台大實驗林進行資安健診惡意網域與IP偵測

- 10Mb/s -> 22Gbytes/5hr (10Mbit /8 X 60s X60m X 5hr)
- 改用 NetFlow 方式儲存



具體辦理事項-資安服務

110年度資安服務維運具體辦理事項：

✓協助台大實驗林進行資安健診惡意網域與IP偵測

- 半天時間(7:30 ~ 12:30)約99MB


```
┌──(yenlchen㉿kali)-[~]
└─$ nfdump -R nfdump -f iplist.txt
Date first seen          Event  XEvent Proto      Src IP Addr:Port          D
st IP Addr:Port     X-Src IP Addr:Port        X-Dst IP Addr:Port   In Byte Ou
t Byte
Summary: total flows: 0, total bytes: 0, total packets: 0, avg bps: 0, avg pp
s: 0, avg bpp: 0
Time window: 2021-03-11 09:47:57 - 2021-03-11 15:11:10
Total flows processed: 0, Blocks skipped: 0, Bytes read: 103813038
Sys: 0.133s flows/second: 0.0        Wall: 0.132s flows/second: 0.0
```

具體辦理事項-網路管理

110年度網路管理維運具體辦理事項：

✓舉辦教育訓練研討會

於10/12日舉辦資安教育訓練，議題分別教育單位弱點檢測平台介紹、破解 IPv6 隱私設計之實作管理經驗。

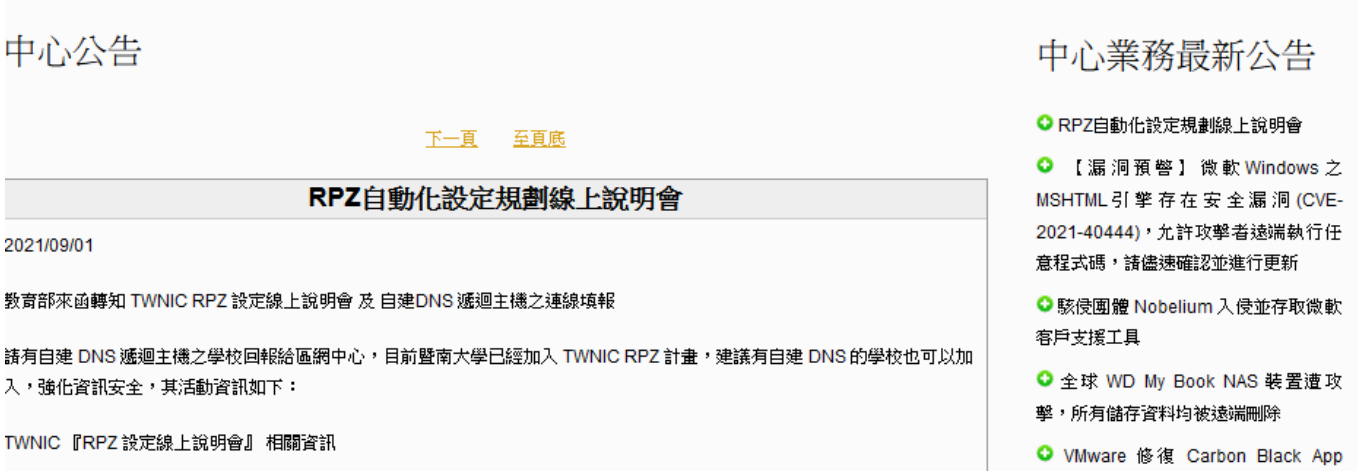
具體辦理事項-資安服務

110年度資安服務維運具體辦理事項：

✓協助暨大附中內部稽核

✓ISMS 驗證導入：本中心及骨幹網路已於本年 1月18日通過教育體系資通安全驗證。

✓區網首頁公告資安相關資訊，包含區網研討會資訊、資安相關議題及新聞，首頁資訊如連結 https://www.ntrc.edu.tw/。



具體辦理事項-網路管理

111年度資安服務目標：

(一)　持續執行110年度項目。

(二)　持續參加 ASOC 中心計畫。

(三)　每年協助連線單位網頁進行 2次 弱點掃描，必要時連線單位可提出增加掃描次數。

(四)　協助縣網中心（含其轄下連線單位）及本中心連線單位弱點掃描報告解讀。

(五)　提供諮詢及協助連線單位導入 ISMS 及完成資安法所要求規定事項，例如內部稽核。

(六)　提供連線單位資安健診惡意網域與 IP 偵測服務。

(七)　配合資訊及科技教育司，進行資安通報及相關資安演練，並於期限內完成連線單位資料整備（密碼更新、聯絡資訊更新），並於演練期間協助連線單位完成通報演練。

未來營運計畫-特色服務

110年度服務特色辦理成效：

IPv6 推廣服務將協助連線單位建置 IPv4/IPv6 Dual-Stack 環境，例如：校首頁支援 IPv6 程度、DNS IPv6 相關設定、IPv6 網段分配及管理建議、IPv4/IPv6 資安軌跡紀錄及收集、IPv6 相關教育訓練等

連線單位14間（不包含台大實驗林分部）		
項目	完成間數	完成率
實地環境現況及訪談	14	100%
區網端IPv6 設定	14	100%
Web Server IPv6設定	11	79%
Web Server支援IPv6正解	11	79%
網頁取樣分析	5	36%

未來營運計畫-特色服務

110年度服務特色辦理成效：

協助偏鄉課輔計畫，小學端及大學端電腦教室硬體、軟體及網路環境維護，本年度服務的單位有都達國小、法治國小、仁愛國小、力行國小、太平國小及瑞峰國中、同富國中。

未來營運計畫-特色服務

110年度服務特色辦理成效：

綠色機房建置：暨南大學海拔 665 公尺，夏季溫度介於 32~24℃，冬季介於 23~15℃，寒流來襲甚至低於 10℃以下，在如此條件下，實施節能減碳規劃，冬季將採外氣引入機制，在氣溫低於 20℃時啟動外氣引入，此系統為一台 5HP 馬力的鼓風機及其外側設置 3 層濾網，搭配 80*40 公分風管，將外部冷空氣均勻導引機房內，目前中心機房整年度PUE值可達 1.22~1.62。

未來營運計畫-特色服務

110年度服務特色辦理成效：

✓協助 ISMS 導入及資安法應辦事宜，例如： ISMS 導入及經驗分享、連線單位內部稽核、資安健診。

✓協助連線單位資安通報事件查詢：針對連線單位資安通報進行各別分析，並將分析結果與可行解決方法告知單位承辦人員，降低被重複通報機率。

MALWARE-CNC Win.Trojan.Gh0st variant outbound connection	175.183.62.229 為站點防火 163.22.186.196 為unifi wifi a 正常傳輸	誤報
MALWARE-CNC Win.Trojan.Agent variant outbound connection	ams 字串	應該為誤報
MALWARE-CNC Win.Adware.Taplika toolbar download attempt	start.mysearchdial.com	https://malwaretips.com/blogs/start-mysearchdial-removal/
MALWARE-CNC Win.Adware.Taplika toolbar download attempt	start.mysearchdial.com	已請老師移除程式
MALWARE-CNC Win.Adware.Taplika toolbar download attempt	start.mysearchdial.com	
MALWARE-OTHER Trackware relevantknowledge runtime detection	User-Agent: OSSProxy 1.3.338.320 Host: rules.securestudies.com https://www.hybrid-analysis.com/sample/4f903d8a4abefdf94b17d16c46490acfe91f84f8bbe74156f9974e http://cleanbytes.net/relevant-knowledge-what-is-it-how-it-get-installed-and-how-to-remove-it https://user-agents.net/string/ossproxy-1-3-338-320-build-338-320-win32-en-us-apr-9-2020-18-44-54	

未來營運計畫-特色服務

111年度創新服務目標與構想：

✓持續協助偏鄉課輔計畫小學端及大學端電腦教室硬體、軟體及網路環境維護。

✓持續協助連線單位資安通報事件查詢。

✓協助 ISMS 導入及資通安全法應辦事宜。

✓協助縣網中心（含其轄下連線單位）及本中心連線單位弱點掃描報告解讀。

前年度改進意見項目及成效精進情形

109委員精進建議項目	110精進建議改進情形
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，通報、應變與事件處理時數，通報及事件完成率接成效良好，但資安事件通報審核平均時數：1.07 小時，尚有進步空間。	本年度資安事件通報審核平均時數：0.05小時，通報應變時數已精進。
提高 IPv6 設定率，推動 IPv6 Dual-Stack 環境已有部分成效，建議可訂定全部連線單位完成期限或其困難點，以期早日將此工作告一段落IPv6 推廣服務為南投區網重要特色服務，目前亦受教育部專案委託推動，建議後可主動收納各區網推動 IPV6 的問題，並研提解決方案以提升學網IPV6 推廣成效。	南投區網中心所有連線單位的 IPv6 管理者和使用狀況進行逐一訪談並且親自到各校實際了解網路建置狀況，以及彙整多位 TANet 專家學者給予的建議，最終將其結果提交給教育部做為未來 IPv6 推動依據。

前年度改進意見項目及成效精進情形

109委員精進建議項目	110年精進建議改進情形
110 年度之營運目標已訂定量化之 KPI 值，但其數值皆偏低，建議可依短期計畫方式訂定整體完成期限，逐年完成。	依委員建議修改其量化指標 https://www.ntrc.edu.tw/achievement.html
目前高中職學校之連線頻寬大部分為100Mbps，建議可參考桃園區網模式，與中華電信等談判，在租金不變下將頻寬提升為300Mbps，可提升高中職之網路使用環境。	桃園區網運作模式似乎較不適合本區網，且多方和中華電信商討，價格調整也不盡理想，故許多連線單位轉換成中投有線介接。
針對 DNS 版本更新報告中似乎著墨不多，建議將其列出，並訂定完成期限已逐年實施，DNS 向上集中的服務。	目前國立高、中職校已由成功大學統一集中管理，南投區網協助連線單位進行網頁弱點掃描，讓連線單位達到可集中標準，順利集中至成功大學。

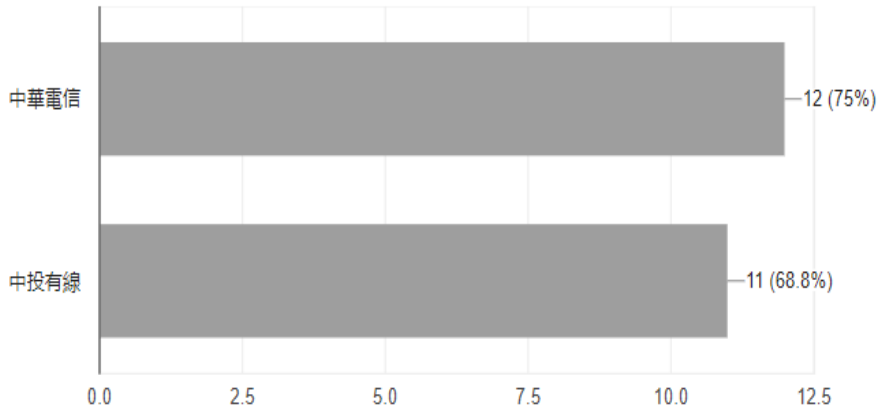
前年度改進意見項目及成效精進情形

109年委員精進建議項目	110年精進建議改進情形
教育訓練的部分可以強化在實務能力提升的指標設定與達成，提升資安防護技術。	礙於疫情影響本年度沒有上機實作課程，但在教育訓練加強實作介面的介紹和操作，並於訓練後進行測驗，看課程內容是否有成效。

滿意度調查（更新中）

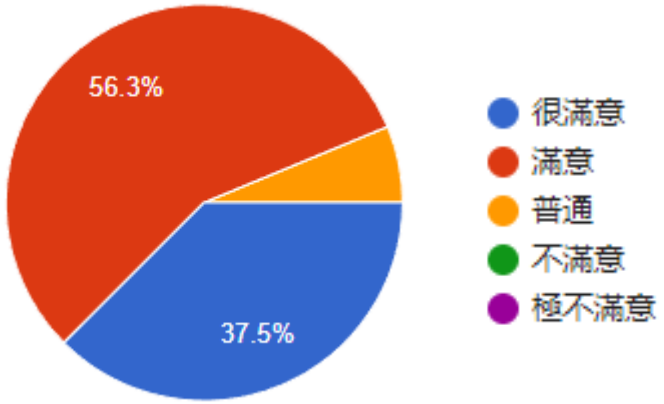
問卷全部連線單位皆完成填寫(台大實驗林分部由台大實驗林本部填寫) 回收率100%

電信業者比例



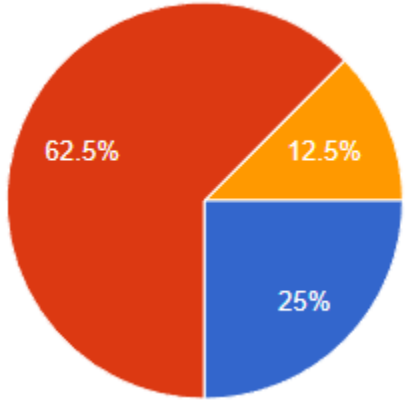
電信業者(ISP)線路穩定度

滿意度



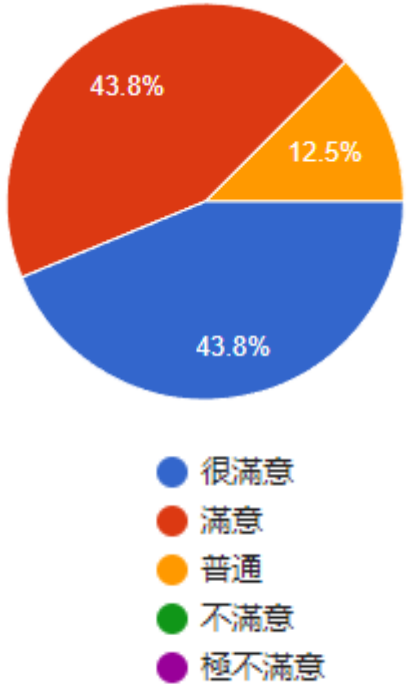
電信業者(ISP)維修速度

滿意度



滿意度調查

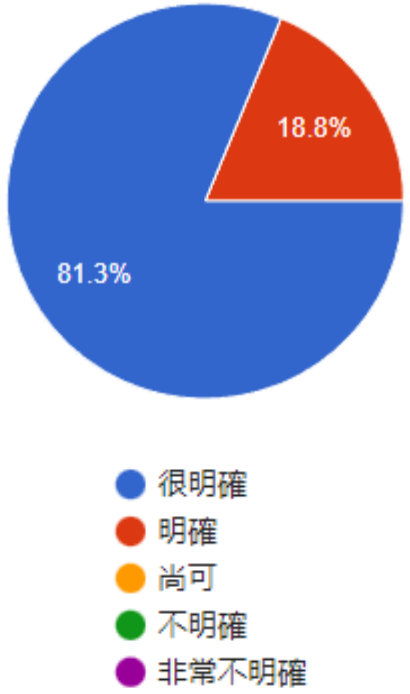
電信業者(ISP)服務態度滿意度



區網人員協助處理資安通報時效滿意度

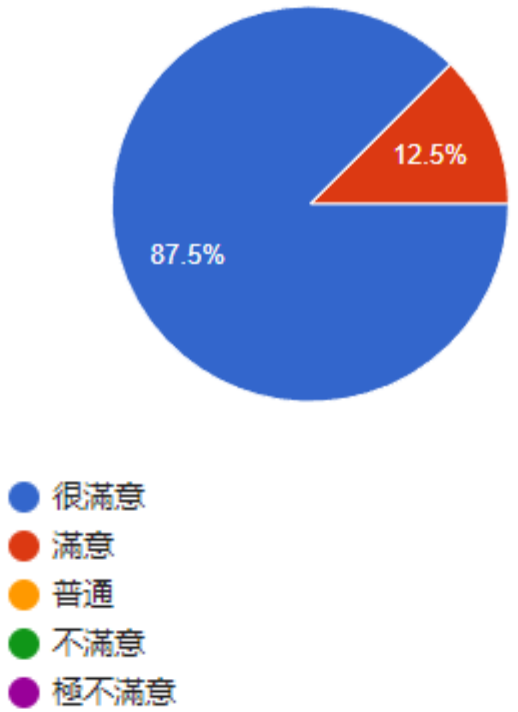
區網人員整體服務滿意度

您是否明確知道區網聯絡窗口

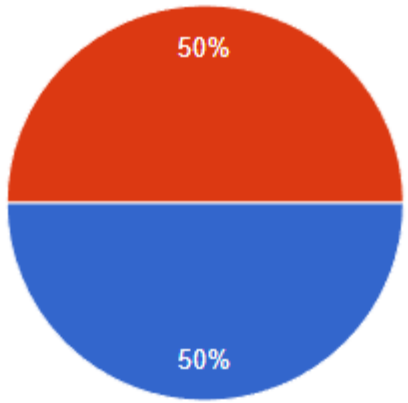


滿意度調查

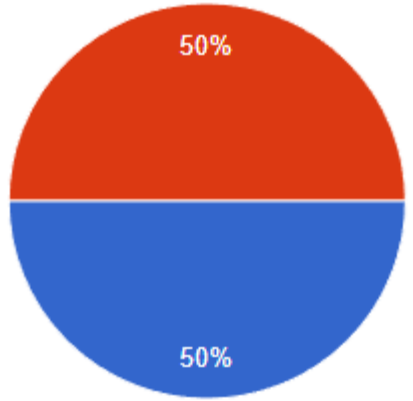
教育訓練議程安排滿意度



未來是否需要區網協助各單位資安內部稽核



是否需要區網其他資安相關協助



- 資安健診
- 資安相關資訊
- 弱點檢測報告分析

報告結束

感謝大家聆聽