

112 年度「臺灣學術網路(TANet)區域網路中心基礎維運與資安人員計畫」

南投區域網路中心

111 年 12 月 12 日

## 112 年度區域網路中心基礎維運計畫內容索引

|                          |           |
|--------------------------|-----------|
| <b>壹、計畫基本項目</b> .....    | <b>3</b>  |
| 一、 計畫期程.....             | 3         |
| 二、 計畫執行單位.....           | 3         |
| <b>貳、計畫執行內容</b> .....    | <b>4</b>  |
| 一、 現況說明.....             | 4         |
| 二、 網管及資安人力服務事項.....      | 5         |
| 三、 網管服務.....             | 5         |
| 四、 資安服務.....             | 14        |
| 五、 特色服務.....             | 16        |
| <b>參、預期效益與精進建議</b> ..... | <b>17</b> |
| 一、 預期效益 KPI： .....       | 17        |
| 二、 去年度精進建議與改善措施.....     | 18        |
| <b>肆、經費需求</b> .....      | <b>20</b> |

## 壹、計畫基本項目

### 一、計畫期程

本計畫期程於 112 年 1 月 1 日起 至 112 年 12 月 31 日止。

### 二、計畫執行單位

由國立暨南國際大學 計算機與網路中心 為主要執行單位。

計畫主持人蕭桂森，教育部補助兩位計畫人員陳彥良、劉育瑄負責區網中心維運及相關業務。

註：人員異動，以最新為主

## 貳、計畫執行內容

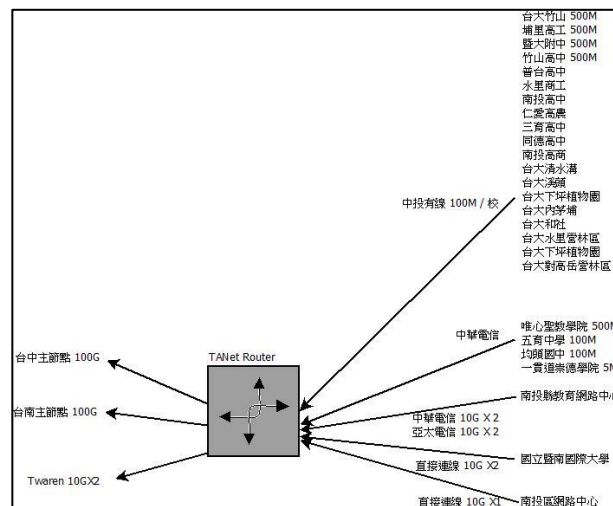
### 一、現況說明

國立暨南國際大學設校於南投縣埔里鎮，為最靠近全國地理中心的一所大學。北連霧社、奧萬大、合歡山，南接日月潭、溪頭、新中橫。校地約一百五十公頃，全區寬廣遼闊。暨大設校，僑教是使命，也是特色。每年負責全國海外聯招，和東南亞國家合作雙聯學制跨國遠距教學。除此之外，本校為南投縣之最高學府，電腦與網路技術之人才濟濟，也因此提供了南投縣地區高品質的網路與電腦技術服務，提昇南投地區的科技發展，縮短城鄉數位落差。

本校計算機與網路中心為台灣學術網路 (TANet) 南投地區之區域網路中心，負責南投縣、市之大專院校、高中職、縣市網中心、研究單位及社教機構連接 TANet 相關事宜，並設置專職網管人員，在最快的時間內解決連線單位之網路問題。

本中心每年邀請各連線單位代表召開一至二次區網管理委員會，討論區網中心管理運作事宜。另外，為推廣最新網路技術並促進經驗交流，每季至少辦理一次網路相關的研討會，邀請連線單位參加，透過區網中心的服務，期能為 TANet 南投地區之使用者提供最佳的網路環境。

南投區網中心現以 Cisco ASR9010 雙實體 100G 線路分別接入台中與台南主節點。目前本區網中心轄下共有 25 個連線單位，其中包含 3 所大專院校、11 所高中職、南投縣網、均頭國中與台大實驗林及其 8 個分部，以下為網路架構圖：



(圖一)、 南投區網中心 TWAREN/TANET 網路架構圖

## 二、網管及資安人力服務事項

- (一) 骨幹網路監測及故障排除
- (二) 資訊安全通報之通報、應變、審核及資訊安全事件資料收集及分析
- (三) 計畫經費控管及計畫行政業務
- (四) ISMS 系統導入及驗證、資通安全法導入
- (五) 南投區網網頁管理
- (六) 配合教育部進行資訊安全通報演練、社交工程演練、業務持續作業演練計畫
- (七) 舉辦教育訓練及連線單位管理委員會
- (八) IPv6 相關業務推廣
- (九) TAnet Roaming 相關業務推廣
- (十) 機房環境監測及電力設備維護
- (十一) 提供連線單位技術協助及各事項反應及聯絡窗口
- (十二) 協助連線單位 DDoS 攻擊流量清洗申請
- (十三) 協助連線單位 ISMS 內部稽核
- (十四) 協助連線單位弱點掃描
- (十五) 協助連線單位資訊安全健診
- (十六) 提供連線單位技術協助及教育部臨時交辦事項

## 三、網管服務

- (一) 提供南投區網中心入口網站 [www.ntrc.edu.tw](http://www.ntrc.edu.tw)



南投區域網路中心  
Nantou Network Regional Center

首頁 資安政策 業務職掌 中心公告 斷線公告 網管資訊 連線單位 研討會資訊 會議記錄 表單下載 相關法規 服務量化指標 常見問題集 歷年成效

中心公告

中心業務最新公告

- RPZ自動化設定規劃線上說明會
- 【漏洞預警】微軟 Windows 之 MSHTML 引擎存在安全漏洞 (CVE-2021-40444)，允許攻擊者遠端執行任意程式碼，請儘速確認並進行更新
- 駭團團體 Nobelium 入侵並存取微軟

RPZ自動化設定規劃線上說明會

2021/09/01

教育部來函轉知 TWNIC RPZ 設定線上說明會 及 自建 DNS 透過主機之連線填報

(圖二)、 區網網頁截圖

網頁內容包含：

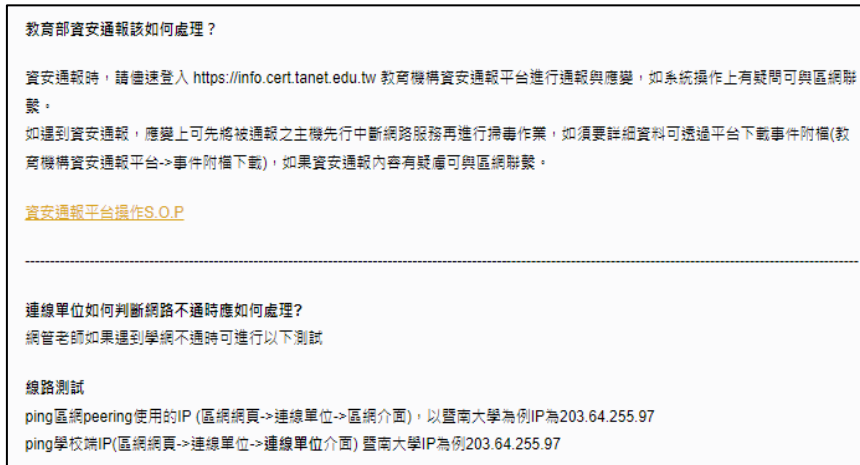
1. 本校資訊安全政策公告
2. 區網人員業務執掌
3. 網頁不定期公告斷線及網路維護資訊
4. 資訊安全相關新聞及漏洞公告
5. 連線單位資訊
6. 研討會資訊
7. 歷年區網管理委員會會議記錄
8. 相關表單下載
9. 資訊安全相關法規
10. 服務量化指標
11. 常見問題集

| 研討會資訊  |
|--|
| [111.08.31][111.09.16] <a href="#">Google帳號兩步驟驗證設定、表單權限及共用安全性設定、開源軟體ODF轉檔技巧</a><br>請來信取得課程錄影檔案 yhliu@ncnu.edu.tw                 |
| [110.05.11][111.05.16] <a href="#">當前網路詐騙案例探討、ISMS 未來推動說明及 資訊系統與資訊資產盤點</a><br>請來信取得課程錄影檔案 yhliu@ncnu.edu.tw                      |
| [110.10.12] 『110年度區網中心管理委員會暨資安教育訓練』 <a href="#">議程</a> 、 <a href="#">教育單位弱點檢測平台介紹</a> 、 <a href="#">破解 IPv6 隱私設計之實作管理經驗</a>      |
| [109.10.26] 109年度教育體系單一登入服務南投縣推廣研習 - <a href="#">老師的課堂神助手 -- Google Classroom</a> 、 <a href="#">Google 教學影音平台大觀與編輯製作教學應用數位教材</a> |

(圖三)、 研討會資訊網頁截圖

| 南投區網中心管理委員會 會議記錄   |
|--|
| [2022.10.14] <a href="#">南投區域網路中心管理委員會 111年度第一次會議紀錄 簡報</a> |
| [2021.12.28] <a href="#">南投區域網路中心管理委員會 110年度第二次會議紀錄 簡報</a> |
| [2021.10.12] <a href="#">南投區域網路中心管理委員會 110年度第一次會議紀錄 簡報</a> |
| [2020.12.08] <a href="#">南投區域網路中心管理委員會 109年度第二次會議紀錄 簡報</a> |
| [2020.07.06] <a href="#">南投區域網路中心管理委員會 109年度第一次會議紀錄 簡報</a> |

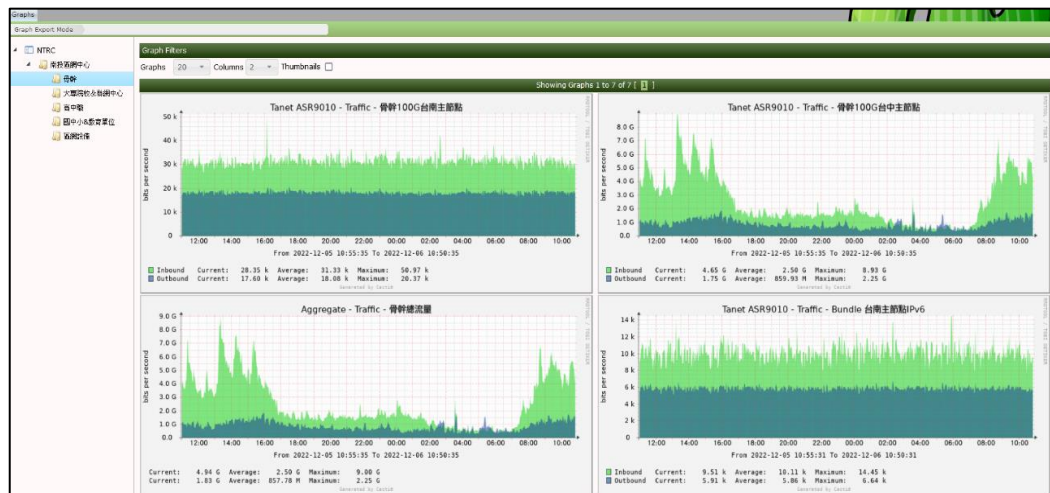
(圖四)、 歷年管理委員會網頁截圖



(圖五)、 常見問題及截圖

(二) 南投區網中心網域名稱服務系統(DNS Server)

(三) 提供 cacti 可回溯的流量紀錄與查詢，可看到各連線單位每日 (1 分鐘統計一次)、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/>



(圖六)、 連外流量統計報表

(四) What's UP 網管監控軟體：

使用 What's UP 網管軟體監測骨幹上各設備效能與連外反應狀態，目前有監控骨幹路由器 ASR9101、骨幹分流設備、機房 UPS 等，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，提供可用率(Availability)、回應時間(Response Time)與斷線告警。



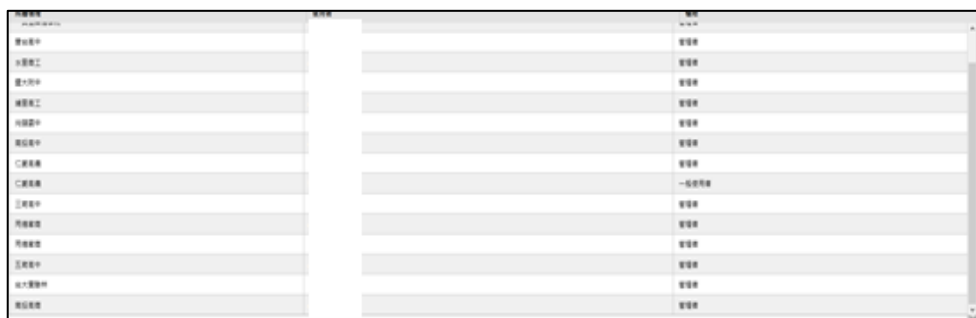
(圖七)、 區網中心 What's UP 網管軟體圖

(五) 提供 NetFlow 查詢系統並開放給連線單位使用：

為了能掌握網路詳細流量狀況使用 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，另外也可透過 N-Reporter 統計功能，進行各單位流量排名，當流量壅塞時找出異常使用 IP



(圖八)、 NetFlow 流量分析與統計

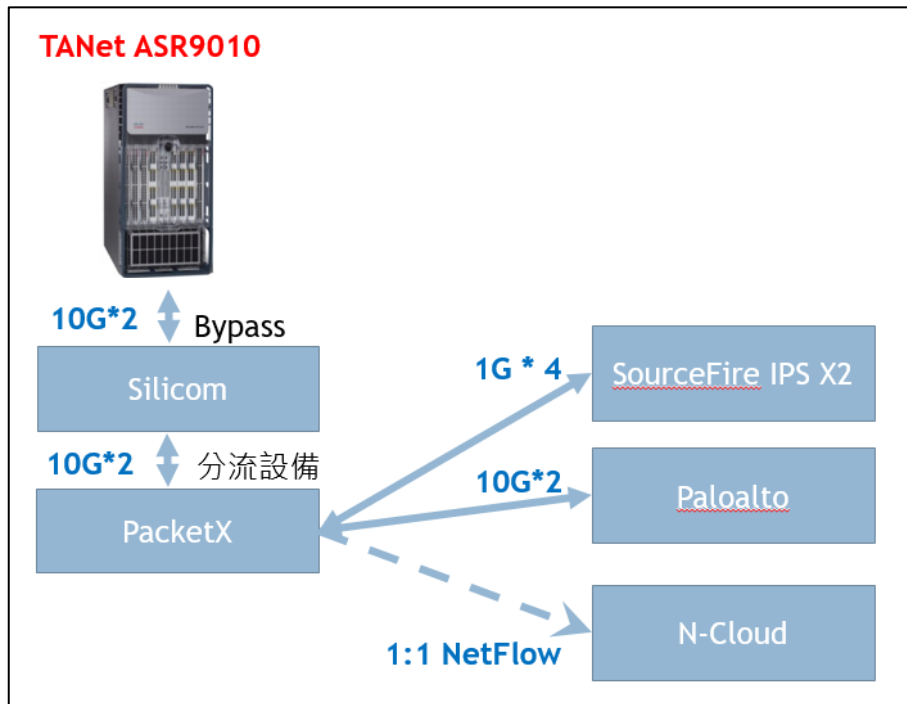


(圖九)、 NetFlow 平台使用權限圖

(六) 分流設備：目前區網裝設有分流設備目前有三個主要作用

1. 過濾加密流量，降低資安設備負擔。
2. 產生 1:1 NetFlow。
3. 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。





(圖十)、資安架構圖

(七) 提高 IPv6 設定率，推動 IPv6 Dual-Stack 環境，南投區網共有 16 間連線單位（包含台大實驗林分部-竹山辦公室），IPv6 使用比率 62.5%，未來將持續推廣 IPv6 服務。

(八) 每年召開兩次連線單位管理委員會

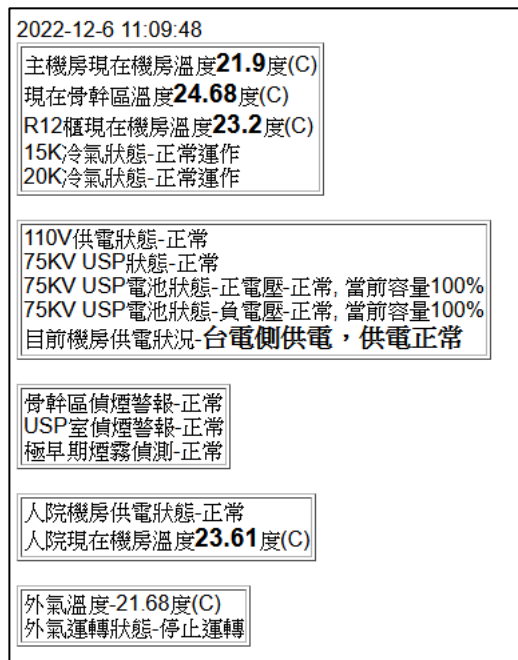
(九) 機房監控與管理

1. 門禁：

本中心依 ISMS 規定進行機房門禁管制，中心人員需刷職員證進入機房，校外人員需填寫相關表單才能進入機房。

2. 溫濕度：

本中心依 ISMS 規定機房溫度應維持在 20°C 至 28°C，相對濕度應維持在 35%RH 至 65%RH，機房溫濕度異常時將會發出簡訊及電子郵件告知。



(圖十一)、 機房環境即時監控網頁

3. 漏液偵測：  
機房內設有大樓水冷主機兩座與氣冷式冷氣兩座，於冷氣旁設有漏液偵測設備，當漏水時可以第一時間發送告警簡訊通知維運人員。
4. 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。
5. 極早期火災預警系統：  
是一種靈敏度非常高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。



(圖十二)、 極早期火災預警系統

6. UPS 不斷電系統：

100G 骨幹使用 SMR 直流供電系統，採雙 AC 回路，機房建置 75K 不斷電系統 (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。



(圖十三)、 75 KVA-UPS 不斷電系統



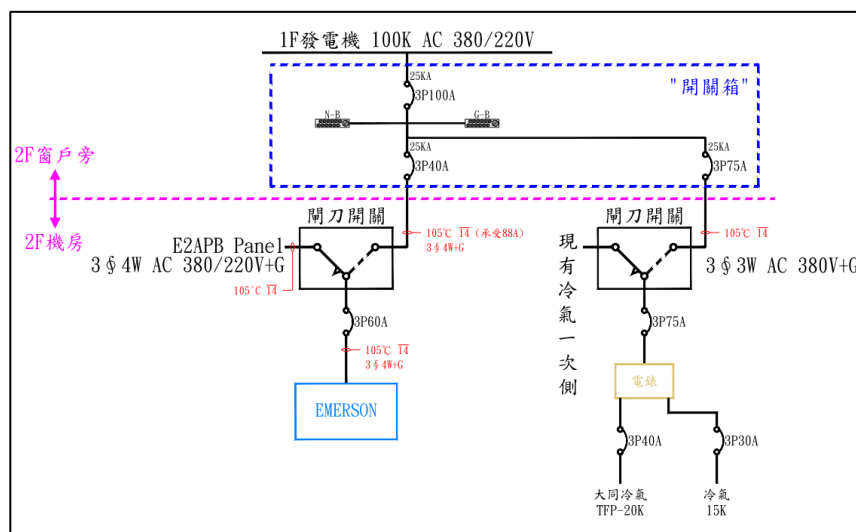
(圖十四)、 75 KVA-UPS 不斷電系統電池箱

7. 市電及發電機保養：

本中心配合學校每年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。

8. 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110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。



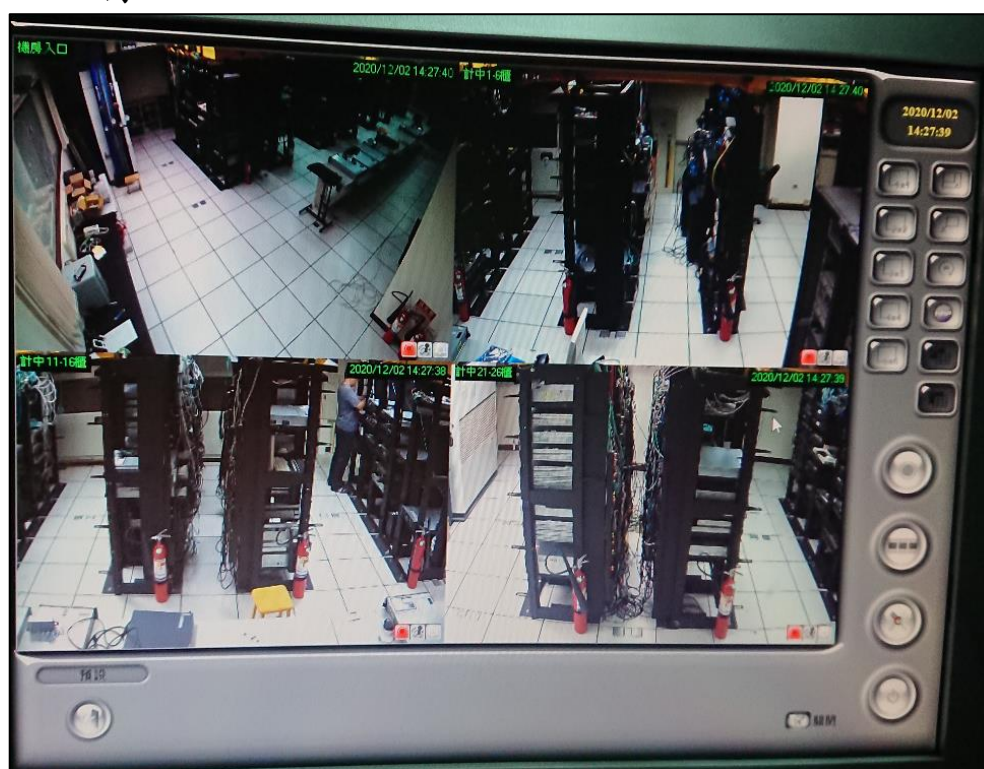
(圖十五)、 第二迴路發電機-配電圖

9. 建置連線單位 LINE 群組，提供便捷快速的分享及交流空間。
10. 空調：  
機房空調部份共有三套系統除原有大樓冰水主機為最後備援外另有兩套空冷主機與 6HP 的自然進氣系統(Free Cooling System)。



(圖十六)、 自然進氣系統

11. 影像監控系統：  
目前機房內已有完善的影像監控系統，管理者能透過網頁直接連線觀察機房內的影像，此外影像也能夠儲存至少 6 個月以上，以供查詢。



(圖十七)、 影像監控系統

#### 四、資安服務

(一) 參與北區 ASOC 中心計畫：

本中心參加 ASOC 中心計畫，北區 ASOC 中心於區網建置兩台 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。

(二) 骨幹 IDS 偵測：

建立網路安全防範機制，目前區網中心的出口已建置 Paloalto 防火牆並啟動 threat 模組，放置於區網出入口進行流量威脅監控，以達到更完善的偵測機制。

(三) 提供網頁弱點掃描平台服務 (<https://evs.twisc.ncku.edu.tw/>)，協助連線單位網頁弱點掃描服務，每年一次，但可視情況增加掃描次數。

| 日期         | 事項  |
|------------|---|
| 2022-05-27 | EVS平台因掃描授權轉換，於2022/05/30 9點起暫停服務<br>預計5/31恢復服務，不便之處，敬請見諒！ |
| 2022-04-14 | 1.檢測排程申請功能已恢復。<br>2.每日新增權限額調整為6個。                         |
| 2022-04-12 | 今日15:00-17:00因服務更新，暫時停止服務。<br>造成不便，敬請見諒。                  |

(圖十八)、 弱點掃描平台

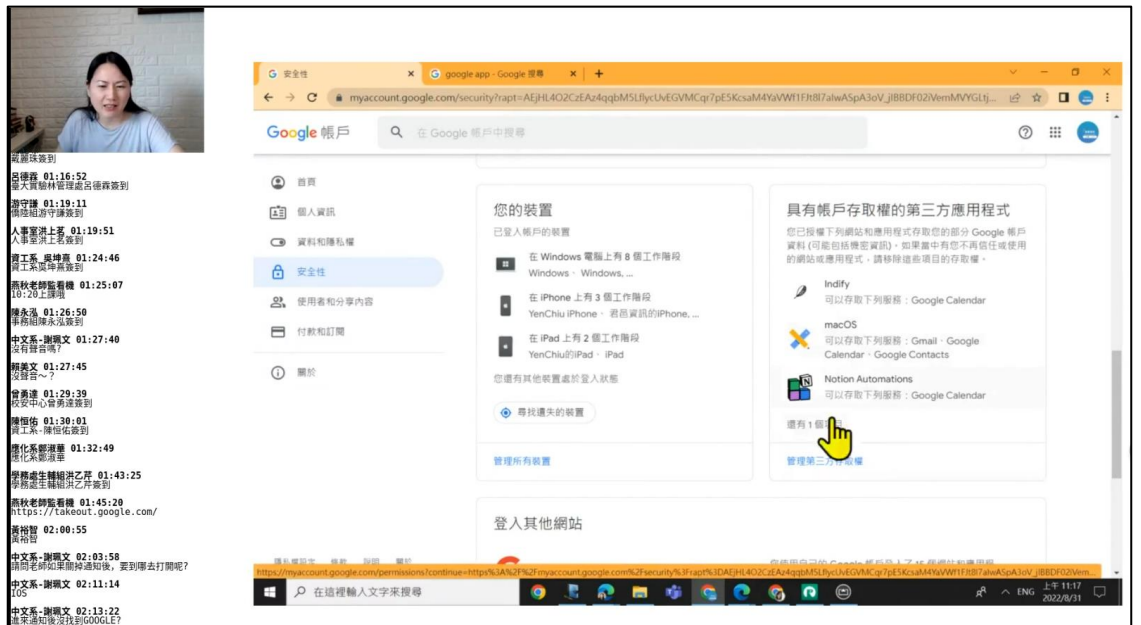
(四) 資安通報：

遵行資通安全事件通報及應變辦法辦理，111 年南投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，數據如下：

- 通報平均時數：0.073 小時
- 應變處理平均時數：0 小時
- 事件處理平均時數：0.6 小時
- 通報完成率：100%
- 事件完成率：100%
- 資安事件通報審核平均時數：0.06 小時
- 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：93.3%

(五) 舉辦教育訓練研討會：

研討會資訊如連結 <https://www.ntrc.edu.tw/conference.html>



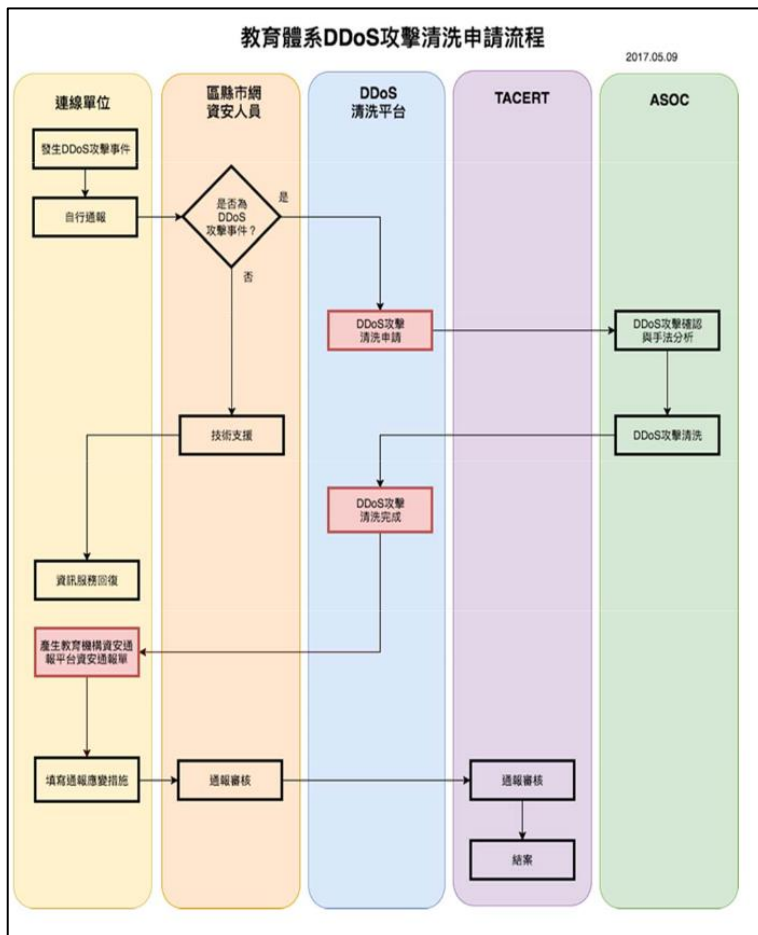
(圖十九)、 線上教育訓練

(六) 協助連線單位進行資安健診：

- 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 和 Domain
  - 透過 mirror port 產生 NetFlow 收集 IP 資訊
  - 透過 mirror port 擷取封包，測錄用戶端詢問 DNS 資訊
- 系統弱點掃描
  - 使用 Nessus 進行系統弱點掃描並提供相關改善方法與建議

(七) 提供連線學校相關資通安全技術與事件之協助處理：南投區網中心平時與各連線單位窗口負責人，保持電話、E-mail 與通訊軟體聯繫，並於區網網頁上轉知教育部各項政令，並提供相關技術諮詢服務。

(八) 分散式阻斷服務通報應變作業



(圖二十)、 DDoS 通報應變作業指引

## 五、特色服務

(一) 連線單位需要時協助網路健檢服務:

由於資安事件層出不窮，如連線單位有技術需求時，將由區網中心派一組人員前往連線單位，瞭解各連線單位網路環境及架構，協助環境檢測及硬體設定，提供技術層面支援，降低資訊安全風險。

(二) 輔導偏鄉國中小進行「數位學伴」:

南投縣內有許多的偏鄉國中小，其教育資源極度缺乏，本區網中心將配合教育部「數位學伴線上課業輔導服務計畫」，本年度的具體工作項目包括協助 JoinNet 設備及硬體維護及加強網路品質，維持一定頻寬。





(圖二十一)、 數位學伴計畫設備維護

### (三) 協助連線單位資安通報查修

中心針對下游連線單位的資安通報進行分析，並見意最佳的處理方式，以防資安事件重複發生。

### (四) 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。

### (五) 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。

## 參、預期效益與精進建議

### 一、預期效益 KPI：

(一) 骨幹網路妥善率達 99%。

(二) 機房空調 PUE 值年平均低於 1.5。

(三) 辦理研討會：

每年至少舉辦 1 場資安教育訓練，議題內容視教育部推動政策及連線單位實際需求調整。

(四) 管理委員會 2 次管理委員：

會議紀錄及相關文件將放置區網網站

(<http://www.ntrc.edu.tw/meeting.html>)

(五) 協助 2 間連線單位 IPv6 環境建置及推廣。

(六) 協助 2 間連線單位進行資安相關服務，例如：資安健診、資安內部稽核或 ISMS 文件審閱等（視連線單位需求安排）。

(七) 協助連線單位資安通報查修。

(八) 針對連線單位進行區網滿意度調查。

(九) 協助連線單位做弱掃報告解讀。

(十) 協助至少 3 間數位學伴小學端電腦軟硬體設備檢修

## 二、去年度精進建議與改善措施

| 111 年精進建議改進情形   | 112 年精進建議改進情形  |
|---|--|
| 區網維運，單位配合費用較為不足，建議適度提高有利業務推展                            | 礙於人事費用佔區網費用大部分經費，雖無提撥配合款，但煩舉辦教育訓練、出差旅費、課程費用、歲修發電機租用、計畫相關耗材等皆由計網中心經費支應。           |
| 維運人員集中 2 人，相較其他區網同樣連線單位之區網，相對應人力建議應達三人                  | 112 年度計畫人力維持配置兩人，人力上相對吃緊，故暫請計中人員支援，希望後年計畫可以配置三名人力。                               |
| 防火牆、IPS(Paloalto)所提供效益並未顯示。                             | Paloalto 已使用超過 10 年，100G 骨幹升級後平寬接近設備效能上限，已於 110 年調整為 IDS 模式，且因設備版本老舊已無法產出相關效益資料。 |
| 應辦理每年區網連線學校基礎資料重新評核與審查。                                 | 依委員建議執行。   |
| 資安事件處理，通報及處理時限內績效皆良好，惟事件處理平均時數 0.6，資訊完整度為 93.33%，建議改善之。 | 依委員建議持續努力。   |

|  |  |
|--|--|
| <p>IPv6 推動完成率為 62.5%，Eduroam 國立學校完成率達 83%，尚可持續努力，建議規劃年限來完成此業務。</p>                   | <p>依委員建議持續努力。</p>  |
| <p>區網管委會於 10/14 召開，惟出席率僅達 65%，出席率偏低，無法達到安政策宣達、經驗分享及收集連線單位意見之會議目的，建議研擬明年如何提高會議出席率</p> | <p>未來預計採實體會議和線上會議並行，並增加討論議題，期以提高出席率。</p>   |
| <p>在滿意度調查中，有些資料列為普通，建議了解並協助解決之。</p>  | <p>滿意度調查中有「普通」的項目為網路連線是否順暢？電信業者(ISP)服務滿意度為何？對電信業者(ISP)維修速度滿意度為何？三個項目，據了解多為 ISP 線路問題造成的滿意度不佳。</p> |
| <p>建議可於每次 BCP 演練時採複合式情境演練，可模擬多種狀況同時發生之應處作業，未來亦可降低事故發生時之應處時間。</p>                     | <p>依委員建議執行。</p>  |
| <p>TACERT 中心每年協助連線單位進行兩次網頁弱掃服務，建議應對弱掃後之高、中風險項目提供改善建議及持續追蹤管考並於辦理第二次弱掃時使用其他弱掃檢測工具</p>  | <p>依委員建議執行。</p>  |

## 肆、經費需求

附件一之一

### 教育部補助計畫項目經費

| 申請單位：國立暨南國際大學                                    |                | 計畫名稱：112 年度「臺灣學術網路 (TANet) 區域網路中心基礎維運與資安人員計畫 |         |           |  |
|--|----------------|--|---------|-----------|--|
| 計畫期程：112 年 1 月 1 日至 112 年 12 月 31 日              |                |  |         |           |  |
| 計畫經費總額：1,635,000 元，向本部申請補助金額：1,635,000 元，自籌款：0 元 |                |  |         |           |  |
| 經費項目   |                | 計畫經費明細                                       |         |           |  |
|  |                | 單價<br>(元)                                    | 數量      | 總價(元)     | 說明   |
| 人事費  | 專任行政助理<br>(網管) | 45,300                                       | 13.5 個月 | 611,550   | 依國立暨南國際大學計畫專任人員薪資基準表辦理，碩士第 7 級薪資 45,300*13.5 月=611,550 (含年終 1.5 個月)  |
|  | 行政助理勞、<br>健保費  | 6,079  | 12 個月   | 72,948    | 勞健保費用依勞基法規定辦理，<br>(勞保 3,848 健保 2,231) *12 個月 =<br>72,948             |
|  | 行政助理勞工<br>退休金  | 2,748  | 12 個月   | 32,976    | 以投保級距金額 45,800，6%為編列上限。<br>2,748*12 個月=32,976                        |
|  | 全民健康保險<br>補充保費 | 1,434  | 一式      | 1,434     | 年終獎金 2.11%之二代健保補充保費<br>45,300*1.5 個月*2.11%=1,434                     |
|  | 專任行政助理<br>(資安) | 46,800                                       | 13.5 個月 | 631,800   | 依國立暨南國際大學計畫專任人員薪資基準表辦理，碩士第 8 級薪資 46,800*13.5 個月=631,800 (含年終 1.5 個月) |
|  | 行政助理勞、<br>健保費  | 6,195  | 12 個月   | 74,340    | 勞健保費用依勞基法規定辦理，<br>(勞保 3,848 健保 2,347) *12 個月 =<br>74,340             |
|  | 行政助理勞工<br>退休金  | 2,892  | 12 個月   | 34,704    | 以投保級距金額 48,200，6%為編列上限，<br>2,892*12 個月=34,704                        |
|  | 全民健康保險<br>補充保費 | 1,481  | 一式      | 1,481     | 年終獎金 2.11%之二代健保補充保費<br>46,800*1.5 個月*2.11%=1,481                     |
|  | 小計             |  |         | 1,461,233 | 專任助理未依上述經費聘用人員致所餘經費不得流用，應依補助比率繳回。                                    |

### 教育部補助計畫項目經費

|  |                  |  |      |           |   |
|--|------------------|--|------|-----------|---|
| 申請單位：國立暨南國際大學                                    |                  | 計畫名稱：112 年度「臺灣學術網路 (TANet) 區域網路中心基礎維運與資安人員計畫 |      |           |   |
| 計畫期程：112 年 1 月 1 日至 112 年 12 月 31 日              |                  |  |      |           |   |
| 計畫經費總額：1,635,000 元，向本部申請補助金額：1,635,000 元，自籌款：0 元 |                  |  |      |           |   |
| 業務費  | 講座鐘點費            | 2,000  | 3 小時 | 6,000     | 研討會及資訊講座鐘點費。講座鐘點費支給表辦理 2000*3 小時=6,000 元。                                   |
|  | 全民健康保險補充保費       | 127  | 一式   | 127       | 6,000*2.11%=127   |
|  | 交通費與住宿費          | 2,000  | 5 次  | 10,000    | 出席會議、資料蒐集、網路健檢、舉辦研習會及研討會之專家學者或人員差旅費及住宿費(依國內出差旅費報支要點辦理)                      |
|  | 膳費               | 100  | 15 人 | 1,500     | 活動及會議膳費，預計辦理整天活動，膳費 100 元/天，約 15 人參加 100*15=1,500                           |
|  | 電腦、通訊、周邊設備之介面、零件 | 3,500  | 一式   | 3,500     | 電腦等相關設備等設備零組件、網路設備介面、軟體、零件單價未達 1 萬元或耐用年限未達 2 年。依「教育部補助臺灣學術網路區域網路中心管理作業要點」編列 |
|  | 雜支               | 2,640  | 一式   | 2,640     | 雜支費用(凡前項費用未列之辦公事務費用屬之。如文具用品、紙張、資料夾、郵資等，單價未達 1 萬元或耐用年限未達 2 年)等依規定編列。         |
|  | 小計               |  |      | 23,767    |   |
| 設備及投資  | 弱點掃描用筆記型電腦       | 45,000                                       | 2 台  | 90,000    | 弱點掃描用高效能記憶體及處理器之筆記型電腦。  |
|  | 網管伺服器            | 60,000                                       | 1 台  | 60,000    | 南投區網，網路管理主機汰換。  |
|  | 小計               |  |      | 150,000   |   |
| 合 計  |                  |  |      | 1,635,000 |   |