111 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 年度區域網路中心基礎維運計畫內容索引

凊	·、計書:	基本項目	3
-			
	- `	計畫期程	3
	二、	計畫執行單位	3
貢	、計畫:	執行內容	4
	- 、	現況就明	
	二、	網管及資安人力服務事項	
	三、	網管服務	
	四、	資安服務	14
	五、	特色服務	18
參	- ` 預期	效益與精進建議	19
	- \	預期效益 KPI:	19
	二、	去年度精進建議與改善措施	19
舄	:、經費	需求	21
	另檢附	· 	教育
	部補助	計畫項目經費申請表。	21

壹、計畫基本項目

一、計畫期程

本計畫期程於111年1月1日起至111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。 目前本單位共有三個組,成員共 20 人,依職責協助區網中心維運。 中心主任:黃育銘

主要團隊

網路組 組長:劉震昌

網路組 組員:陳彦良、劉育瑄、楊文龍、楊世偉、陳家祿、張瑛杰、吳

佩璇

次要團隊

系統組 組長:簡文章,組員:王永吉、黎俊彦

諮詢組 組長:陳順德,組員:何奇芳、黃仁弘、黃景煌、

王靖怡、潘依岑、林家琪

註:本中心若有人員異動,以最新為主

貳、計畫執行內容

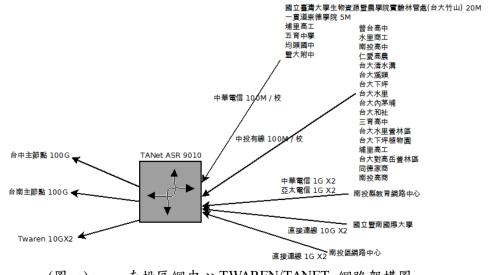
一、現況說明

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、新中横。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,更 藉由網路成立資訊、語文等虛擬教室,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隨時待命,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 23 個連線單位,其中包含 2 所大專院校、10 所 高中職、南投縣網、均頭國中、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) 機房環境監測及電力設備維護
- (十) 提供連線單位技術協助及各事項反應及聯絡窗口
- (十一) 協助連線單位 DDoS 攻擊流量清洗申請
- (十二) 協助連線單位 ISMS 內部稽核
- (十三) 協助連線單位弱點掃描
- (十四) 協助連線單位資訊安全健診
- (十五) 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



(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(教育部資安通報該如何處理?網路不通時應如何處理?)



(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 [2021.10.12] 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 [2020.12.08] 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 [2020.07.06] 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 [2019.11.06] 南投區域網路中心管理委員會108年度第一次會議紀錄 [2018.12.21] 南投區域網路中心管理委員會107年度第二次會議紀錄 [2018.02.05] 南投區域網路中心管理委員會107年度第一次會議紀錄 簡報 [2017.11.10] 南投區域網路中心管理委員會106年度第一次會議紀錄 簡報 [2017.11.10] 南投區域網路中心管理委員會106年度第一次會議紀錄 簡報

(圖四)、 歷年管理委員會網頁截圖

教育部資安通報該如何處理?

資安通報時,請儘速登入 https://info.cert.tanet.edu.tw 教育機構資安通報平台進行通報與應變,如系統操作上有疑問可與區網聯

如遇到資安通報,應變上可先將被通報之主機先行中斷網路服務再進行掃毒作業,如須要詳細資料可透過平台下載事件附值(教育機構資安通報平台->事件附值下載),如果資安通報內容有疑慮可與區網聯繫。

資安通報平台操作S.O.P

連線單位如何判斷網路不通時應如何處理?

網管老師如果遇到學網不通時可進行以下測試

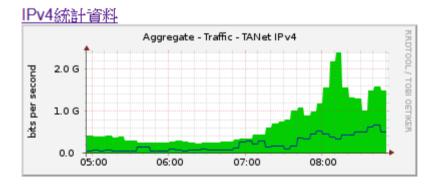
線路測記

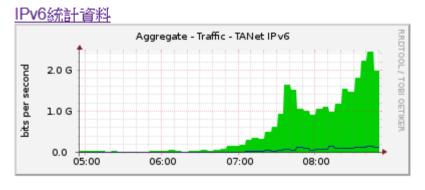
ping區網peering使用的IP (區網網頁->連線單位->區網介面),以暨南大學為例IP為203.64.255.97 ping學校端IP(區網網頁->連線單位->連線單位介面) 暨南大學IP為例203.64.255.97

(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(5分鐘更新一次)、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/traffic3.html

Tanet 100G 骨幹(其他詳細資料)



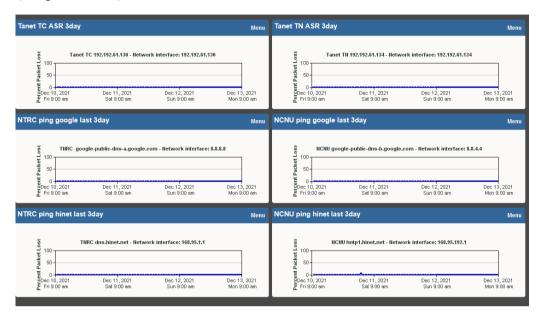


(圖六)、 連外流量統計報表

(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

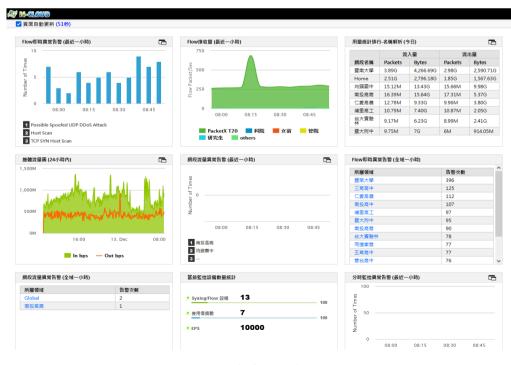
前有有監控骨幹路由器 ASR9101、骨幹防火牆 Paloalto5060、骨幹分流設備 PacketX、機房 UPS 等,另外針對網路有偵測台中主節點、台南主節點、與各連線單位節點狀態,可提供可用率(Availability) 、回應時間 (Response Time)與斷線告警。



(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,當流量雍塞時找出異常使用 IP

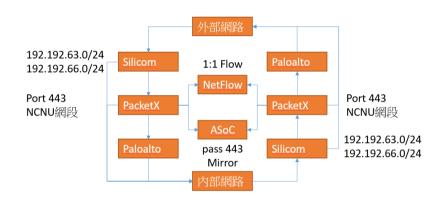


(圖八)、 NetFlow 流量分析與統計



(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. 過濾加密流量進入資安設備降低資安設備負擔。
 - 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 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,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. 温濕度:

本中心依 ISMS 規定機房溫度應維持在 20℃至 28℃ ,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。

2020-12-2 11:36:10

主機房現在機房溫度20.7度(C)
現在骨幹區溫度22.93度(C)
15K冷氣狀態-正常運作
20K冷氣狀態-正常運作
20K冷氣狀態-正常運作
75KV USP狀態-正常
75KV USP默態-正常
75KV USP電池狀態-正電壓-正常
75KV USP電池狀態-直電壓-正常
75KV USP電池狀態-負電壓-正常
75KV USP電池狀態-負電壓-正常
75KV USP電池狀態-負電壓-正常
75KV USP電池狀態-負電壓-正常
75KV USP電池狀態-頁電壓-正常
75KV USP電池狀態-正常
75KV USP電池狀態-正常

(圖十一)、 機房環境異常監控系統

外氣運轉狀態-停止運轉|

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簡訊告警通知維運人員。

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:

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



(圖十三)、 75 KVA-UPS 不斷電系統



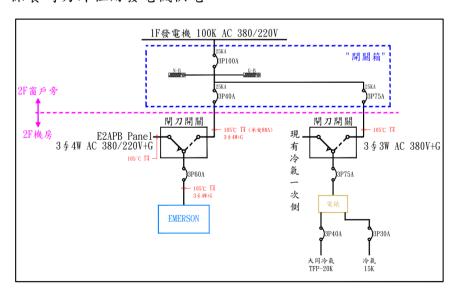
(圖十四)、 75 KVA-UPS 不斷電系統電池箱

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。



(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。



(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3個月以上,以供查詢。



(圖十七)、 影像監控系統

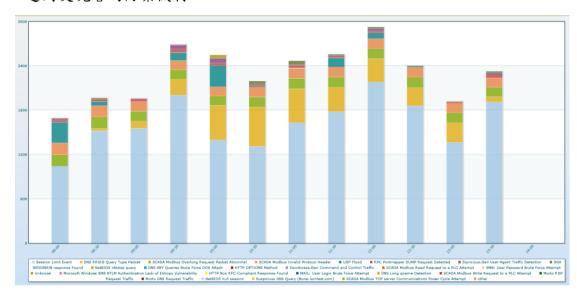
四、資安服務

(一) 參與北區 ASOC 中心計畫:

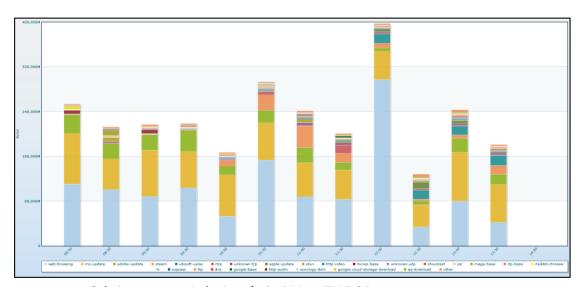
本中心參加 ASOC 中心計畫,北區 ASOC 中心於區網建置兩台 FirePower 入侵防禦系統,並透過 TACERT 台灣學術網路危機處理中心 平台派發資通安全事件。

(二) 骨幹防火牆:

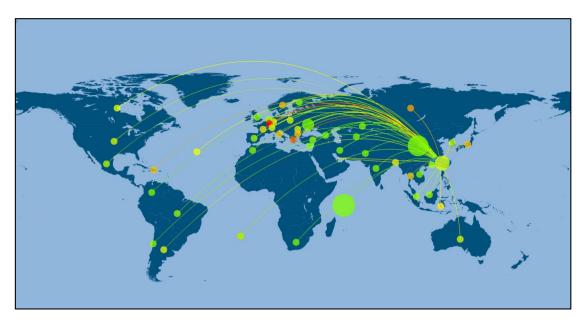
建立網路安全防範機制,目前區網中心的出口已擺置 Paloalto 頻寬管理器 進行頻寬的管理以及部分攻擊抵禦;此外也有 Sourcefire 放置於區網出入口進行流量威脅監控,目前 Sourcefire 設定為 mirror 監控狀態,以達到更完善的防禦機制。



(圖十八)、 網路威脅防禦排行 TOP 25



(圖十九)、 網路應用程式使用排行 TOP 25



(圖二十)、 全球對於本中心網路攻擊來源示意圖

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



(圖二十一)、 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,110年配合教育部資安演練1、2級資安事件處理,成績數據如下:

▶ 通報平均時數: 0.07 小時

▶ 應變處理平均時數: 0.24 小時

▶ 事件處理平均時數: 0.85 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: 100.00%

(五) SMS 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。

(六)舉辦教育訓練研討會:

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



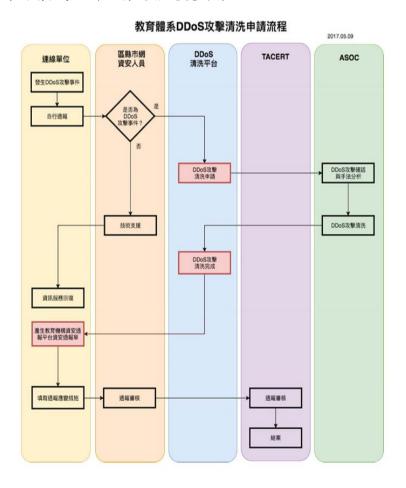
(圖二十二)、 線上教育訓練

- (七)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 & 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

```
0
2021-03-11 15:10:06.466 INVALID Ignore UDP
163.22.2.2:53
0.0.0.0:0 → 0.0.0.0:0 59
0
2021-03-11 15:10:06.140 INVALID Ignore UDP
163.22.2.1:53 → 0.0.0.0:0 → 0.0.0.0:0 435
0
2021-03-11 15:10:06.352 INVALID Ignore UDP
163.22.2.1:53 → 0.0.0.0:0 → 0.0.0.0:0 62
0
2021-03-11 15:10:06.352 INVALID Ignore UDP
163.22.2 1:53 0.0.0.0:0 → 0.0.0.0:0 62
0
2021-03-11 15:10:06.466 INVALID Ignore UDP
163.22.2:53 0.0.0.0:0 → 0.0.0.0:0 66
0
2021-03-11 15:10:10:10 INVALID Ignore UDP
163.22.2:53 0.0.0.0:0 → 0.0.0.0:0 526
0
021-03-11 15:10:10.100 INVALID Ignore UDP
163.22.2.1:53 → 0.0.0.0:0 → 0.0.0.0:0 526
0
2021-03-11 15:10:06.558 INVALID Ignore UDP
163.22.2.1:53 → 0.0.0.0:0 → 0.0.0.0:0 526
0
2021-03-11 15:10:06.558 INVALID Ignore UDP
10.9.26.255:58568 → 163.22.2.1:53 → 0.0.0.0:0 → 0.0.0.0:0 76
0
2021-03-11 15:10:06.558 INVALID Ignore UDP
10.9.26.255:58568 → 163.22.2.1:53 → 0.0.0.0:0 → 0.0.0.0:0 76
0
2021-03-11 15:10:06.558 INVALID Ignore UDP
10.9.26.255:58568 → 163.22.2.1:53 → 0.0.0.0:0 → 0.0.0.0:0 76
0
2021-03-11 15:10:06.558 INVALID Ignore UDP
10.9.26.255:58568 → 163.22.2.1:53 → 0.0.0.0:0 → 0.0.0.0:0 76
0
2021-03-11 15:10:06.558 INVALID Ignore UDP
10.9.26.255:58568 → 163.22.2.1:53 → 0.0.0.0:0 → 0.0.0.0:0 76
0
2021-03-11 15:10:06.558 INVALID Ignore UDP
10.9.26.255:58568 → 163.22.2.1:53 → 0.0.0.0:0 → 0.0.0.0:0 76
0
2021-03-11 15:10:06.558 INVALID Ignore UDP
10.9.26.255:58568 → 10.0.0.0:0 → 0.0.0.0:0 76
0
2021-03-11 15:10:06.558 INVALID Ignore UDP
10.9.26.255:58568 → 10.0.0.0:0 → 0.0.0.0:0 76
0
2021-03-11 15:10:06.558 INVALID Ignore UDP
10.9.26.255:58568 → 10.0.0.0.0:0 → 0.0.0.0:0 76
0
2021-03-11 15:10:06.558 INVALID Ignore UDP
10.9.26.255:58568 → 10.0.0.0.0:0 → 0.0.0.0:0 76
0
2021-03-11 15:10:06.558 INVALID Ignore UDP
10.9.26.255:60981 → 0.0.0.0.0:0 → 0.0.0.0:0 → 0.0.0.0:0 → 0.0.0.0:0 → 0.0.0.0:0 → 0.0.0.0:0 → 0.0.0.0:0 → 0.0.0.0:0 → 0.0.0.0:0 → 0.0.0.0:0 → 0.0.0.0:0 → 0.0.0.0:0 → 0.0.0.0:0 → 0.0.0.0:0 → 0.0.0.0:0 → 0.0.0.0:0 → 0.0.0.0:0 → 0.0.0.0:0 → 0.0.0.0:0 → 0.0.0.0:0 → 0.0.0.0:0 → 0.0.0.0:0 → 0.0.0.0:0 → 0.0.0.0:0 → 0.0.0.0:
```

(圖二十三)、 惡意網域與 IP 偵測資料

- (八) 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。
- (九)分散式阻斷服務通報應變作業



(圖二十四)、 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) 提供網路電話服務,由區網架設 SIP 主機供連線單位使用。
- (三)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。





(圖二十五)、 數位學伴計畫設備維護

(四)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。

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	
MALWARE-CNC Win.Trojan.Agent variant outbound connection	ams 字串	應該為誤韓
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/4f903d8a4abefdf94b17d16c46490acfe91f84f8bbe74156f9974 http://www.hybrid-analysis.com/sample/4f903d8a4abefdf94b17d16c46490acfe91f84f8bbe74156f9974 https://user-agents.net/string/ossproxy-1-3-338-320-build-338-320-win32-en-us-apr-9-2020-18-44-54	

(圖二十六)、 協助連線單位分析資安通報事件

- (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)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場資安研討會或者教育訓練,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eduroam建置。
- (七)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)。
- (八)協助連線單位資安通報查修。
- (九)針對連線單位進行區網滿意度調查。
- (十)協助縣網中心及其連線單位做弱掃報告解讀
- (十一)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

110 年精進建議改進情形	111 年精進建議改進情形
說明網路流量 FirePower 分析成果未說	FirePower為ASOC建置於南投區網設備,
明	後端分析與通報都由 ASOC 負責。
資安健診、惡意檢測成果較為欠缺,報告	本次報告中的資安健診項目為當年度新
可強化對連線單位的網路資安優化之協	增加項目,屬測試性質,於新年度會精進
助	檢測方式與報告呈現內容,以協助連線
	單位加強資安能量。
教育訓練課程可思考數位化保存,且如	區網會擬講師同意書,再透過暨大所提
何就教育訓練之品質加以循環改善。	供的 BBB 系統錄影,並提供給參與人員。
本年度因疫情關係,故教育訓練辦理場	
次較少,建議明年可增加辦理場次。	
建議思考如何協助轄下各級機關學校符	協助連線單位進行資安相關服務,例如:
合資通安全管理法相關要求,若有相關	資安健診、資安內部稽核或 ISMS 文件審
問題亦請了解反應之	閱等 (視連線單位需求安排)
網路監控除 Cacti 及 NetFlow 外,應有	目前 NetFlow 有小時 TOP 流量與即時異
更即時之流量監測機制·此外,應思考是	常告警,Cacti 統計時間為 5 分鐘顯示,

否僅用 Cacti, NetFlow, What's Up 除以上兩套外即時流量監測還可以透過即足以充分滿足監控區網中心所提供之 Router 本身的界面監測 (monitor 各式服務。 interface)得知流量現況,另外 What's

應每年針對網路維運研議新興技術,以 充分呈現持續自我精進之動力

除以上兩套外即時流量監測還可以透過 Router 本身的界面監測 (monitor interface)得知流量現況,另外 What's UP 也可透過 SNMP 針對單一界面做即時 監測並繪製圖表,新興技術部分需再研 擬。

對區網連線單位之協助效益報告不足。 年度成果基礎資料應充分呈現區網中心 當年之維運成效,應以更豐富之文字來 呈現。

感謝委員建議在報告撰寫方面會盡量呈 現,豐富內容。

下年度目標應涵括區網中心下年度目標 應涵蓋區網中心之基礎服務,例如;網路 妥善率,呈現服務品質之自我要求,宜用 更清楚的質化和量化敘述來呈現。 建議明(111)年度計畫訂定明確且較高

標準之 KPI 值,以利業務之推動

於本年度預期效益KPI中呈現。

肆、經費需求

另檢附南投區域網路中心-111 年度台灣學術網路區域網路中心基礎維運與資安人員計畫教育部補助計畫項目經費申請表。

補(捐)助	申請金額	核定計畫金額	核定補助金額	說明
		, -		近 切
項目	(元)	(教育部填列)	(教育部填列)	
		(元)	(元)	
				1. 專任行政助理2人(碩士1人及學士
				1人),本計畫人員共2人。
人事費	1, 391, 258			2. 所編費用含薪資、法定保險費用、 勞退金、年終獎金及其補充保費。
, - 1 %	1, 331, 2 33			3. 補(捐)助款不得編列加班費及應休 未休特別工資。
				4. 未依學經歷(職級)或期程聘用人
				員,致補(捐)助剩餘款不得流用。
				1. 講座鐘點費(含補充保費)、膳費、 交通費與住宿費等依講座鐘點費支
				給規定、二代健保規定、臨時人員
				新資規範及國內出差旅費報支要 點,訂有固定標準給付對象之費
				用。 2. 依國內出差旅費報支要點之相關費
				用。
業務費	58, 742			3. 辦理業務所需,含設備維護費、電 腦、通訊、周邊設備之介面、零件
				等,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。
				4. 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。
				1. 資訊軟硬體設備: 電腦 (桌上或筆
				記型)、平版電腦、伺服器、儲存設 備、環控設備、網路介面模組、網
設備及投資	150,000			路交換器、不斷電系統電池組、空
貝				調設備、發電機及線路、門禁系 統、監視系統等等或資訊相關設 備。(電腦上限3萬元)
				備。(電腦上限3萬元)
合 計	1,600,000			
<u>'</u>	1, 000,000			