南投區域網路中心
期末審查

計算機與網路中心 黃育銘主任

報告人：網路組組長 劉震昌

基礎維運資料

一、經費及人力-經費使用

1.核定計畫金額：1,395,000

2.教育部補助金額：1,395,000

3.實際累計執行數（至11月）：96% 已扣除必要人事費及差旅費

自籌款:320萬購買防火牆設備

基礎維運資料

一、經費及人力-中心人力數

專任：21人　　兼任：2人

其中包含教育部補助

網管人員：1人，證照數：3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）

資安人員：1人，證照數：6張

(ITE 網際網路介接基礎、ITE 資料通訊、ITE 網際網路服務與應用、ITE 網路安全、網路架設乙級技術士技、CHFI 資安鑑識調查專家認證）

基礎維運資料

二、經費使用情形及績效檢討

歷年經費達成率

年度	補助經費（元整）	自籌經費（元整）	年度達成率	備註
105	1,449,866	1,785,600	100%	UPS
106	1,350,000	310,000	99.89%	ATS、人員教育訓練
107	1,390,000	533,000	100%	SMR、ATS、自然進氣
108	1,395,000	3,200,000	96% 至11/7日止(已扣除必要人事費、差旅費)	防火牆

基礎維運資料

三、網管及資安人力之服務績效

在職年度	職缺	姓名	任務配置
98-108	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 ISMS 系統導入及驗證、資安法導入 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 舉辦教育訓練及相關活動 提供連線單位各事項反應及聯絡窗口及其他交辦事項
103-108	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 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

人員異動因素：
網管及資安人力皆在職多年，故沒有異動的問題，歷年人事經費也沒有繳回的問題。

基礎維運資料

四、基礎資料(網管及資安)

(一)　區網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	非學校連線單位	總計
(1)　連線數 (以單位(校)數統計)	單位(校)數		1	2	10	1	9	23
	連線比例		1/23	2/23	10/23	1/23	9/23	單位(校)數 / 總計
(1)　連線頻寬 (以電路數統計)	專線(非光纖)				南投高商			
	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
		500M(含)以上 1G(不含)以下						
		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

基礎維運資料

四、基礎資料(網管及資安)

(一)區網中心連線資訊彙整表

(3)連線縣(市)教育網路中心	縣(市)教育網路中心	連線頻寬(1)	連線頻寬(2)	備註
	1. 南投縣教育處	中華電信1G×2	亞太電信1G×2	
(4)連線其他單位(非ISP)	其他單位名稱	連線頻寬(1)	連線頻寬(2)	備註
	1. 無			
(5)連線TANet及其他ISP線路	臺灣學術網路(TANet)		連線台中主節點頻寬100Gbps	連線台南主節點頻寬100Gbps
(6)補充說明：	無			
(7)連線資訊	請依附表「學校/單位連線資訊詳細表」格式填附			

網路架構圖

國立臺灣大學生物資源暨農學院實驗林管處(台大竹山) 20M
一貫道崇德學院 5M
埔里高工
五育中學
均頭國中
暨大附中
普台高中
水里商工
南投高中
仁愛高農
台大清水溝
台大溪頭
台大下坪
台大水里
台大內茅埔
台大和社
三育高中
台大水里營林區
台大下坪植物園
埔里高工
台大對高岳營林區
同德家商
南投高商
中華電信 100M / 校
中投有線 100M / 校
台中主節點 100G
TANet ASR 9010
台南主節點 100G
Twaren 10GX2
中華電信 1G X2
亞太電信 1G X2
南投縣教育網路中心
國立暨南國際大學
直接連線 10G X2
直接連線 1G X2
南投區網路中心

基礎維運資料

四、基礎資料(網管及資安)

(二)區網中心資訊安全環境整備表

1. 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。(由教育部資科司提供數據)

✓ 1、2級資安事件處理：

(1) 通報平均時數： 1.185小時

(2) 應變處理平均時數： 0.009 小時

(3) 事件處理平均時數：1.194小時

(4) 通報完成率：100%

(5) 事件完成率：98.592%

(6) 資安事件通報審核平均時數： 0.564小時

✓ 3、4級資安事件通報：本年度無3、4級資安通報事件

基礎維運資料

四、基礎資料(網管及資安)

事件完成率：**98.592%**

這兩筆資料是審核時間誤值導致計算出來不符合規定

		發生時間	發佈時間	一線通報	一線應變	二線通報審核	二線應變審核
普台高級中學	系統被入侵	2019-04-01 08:08:00	2019-04-01 09:15:43	2019-04-01 09:50:33	2019-04-01 10:27:44	2019-04-01 10:01:07	1999-01-01 00:00:00
內頭國民中學	殭屍電腦(Bot)	2019-03-07 08:10:00	2019-03-07 08:30:21	2019-03-07 08:30:34	2019-03-07 08:30:34	2019-03-07 08:30:24	2019-03-07 08:30:24

基礎維運資料

四、基礎資料(網管及資安)

(二)區網中心資訊安全環境整備表

(2) 網路中心配合本部資安政策

1. 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 %

2. 區網網路中心依資通安全應執行事項:

(1)是否符合防護縱深要求? ■是 □否

本中心具備防毒、防火牆、郵件過濾系統、IDS/IPS

(2)是否符合稽核要求? ■是 □否

本年度6月25日通過教版新版 ISMS 稽核

基礎維運資料

四、基礎資料(網管及資安)

(二)區網中心資訊安全環境整備表

(2) 網路中心配合本部資安政策

2. 區網網路中心依資通安全應執行事項:

(3)符合資安專業證照人數：8員

ISMS主導稽核員證照8張、個資管理制度證照4張、資安職能評量證書2張、及其他技術相關證照

(4)維護之主要網站進行安全弱點檢測比率：100%

每年針對連線單位進行兩次校首頁弱點掃描，並將掃描報告分析後，提供給有漏洞的連線單位

資安架構圖

外部網路
192.192.63.0/24
192.192.66.0/24
Silicom
1:1 NetFlow
Facebook
Youtube
PacketX
Zone Protection
DoS Protection
Paloalto
Mirror
Sourcefire
Mirror
Paloalto
PacketX
Facebook
Youtube
1:1 NetFlow
Silicom
192.192.63.0/24
192.192.66.0/24
內部網路

網路管理

網路連線、網管策略及具體辦理事項

- **108年度網路管理維運具體辦理事項**

1. VoIP over IPv6 推動：全校已全面改用網路電話系統，已建置1500門，並將區網實體 SIP Server 虛擬化。

區網SIP Server使用量：

本年度用量約4,565 通，約計5,288 分鐘

網路管理

網路連線、網管策略及具體辦理事項

- **108年度網路管理維運具體辦理事項**

  2. 持續提供 NetFlow 查詢系統並開放給連線單位使用。

網路管理

網路連線、網管策略及具體辦理事項

➢ **108年度網路管理維運具體辦理事項**

3. 資安事件：協助查修事件類型及分析，讓連線單位資訊教師能迅速排除問題。

10/17接到連線單位反應發生內部 UDP 攻擊防火牆告警，協請連線單位廠商於防火牆內抓取封包，發現是 DNS 大量封包，來源 IP 多目地 IP 一號，再反查區網 flow 資料發現有一樣的情況，確認來源位置是偽造。

No.	Time	Source	Protocol	Destination	Length	Da
1	2019-10-17 11:18:19.093163	[redacted].24	DNS	[redacted].23	97	
2	2019-10-17 12:03:37.020416	[redacted].39	DNS	[redacted].38	97	
3	2019-10-17 15:25:25.437103	[redacted].1	DNS	[redacted].0	97	
4	2019-10-17 15:49:23.633121	[redacted].59	DNS	[redacted].58	97	
5	2019-10-17 19:09:17.701414	[redacted].29	DNS	[redacted].28	97	
6	2019-10-17 23:00:25.588381	[redacted].54	DNS	[redacted].53	97	
7	2019-10-18 00:13:08.958790	[redacted].18	DNS	[redacted].17	97	
8	2019-10-18 01:12:29.489540	[redacted].31	DNS	[redacted].30	97	
9	2019-10-18 01:23:14.608682	[redacted].8	DNS	[redacted].7	97	
10	2019-10-18 02:02:56.660776	[redacted].53	DNS	[redacted].52	97	
11	2019-10-18 04:03:00.473146	[redacted].41	DNS	[redacted].40	97	
12	2019-10-18 11:01:29.937594	[redacted].10	DNS	[redacted].9	97	
13	2019-10-18 12:27:29.916711	[redacted].43	DNS	[redacted].42	97	
14	2019-10-18 13:11:49.102650	[redacted].6	DNS	[redacted].5	97	
15	2019-10-18 13:47:05.365131	[redacted].22	DNS	[redacted].21	97	
16	2019-10-18 14:26:20.734278	[redacted].32	DNS	[redacted].31	97	

網路管理

網路連線、網管策略及具體辦理事項

- **108年度網路管理維運具體辦理事項**

  4. 協助教育部相關計畫：協助遠距課輔硬體及網路維護，及維持課輔品質。

網路管理

網路連線、網管策略及具體辦理事項

- **108年度網路管理維運具體辦理事項**

5. 提高 IPv6 設定率，15間連線單位（不包含台大分部）有9間完成IPv6 設定，再持續推廣後108年已經有12間完成設定，之後將持續推廣。

已完成單位：南投縣網、暨南大學、埔里高工、暨大附中、水里商工、同德家商 、仁愛高農、三育高中、均頭國中五育高中、南投高商、普台高中

未完成單位：一貫道崇德學院、南投高中、台大竹山實驗林本部

網路管理

網路連線、網管策略及具體辦理事項

➢ **108年度網路管理維運具體辦理事項**

5. 提高 IPv6 設定率，15間連線單位（不包含台大分部）有9間完成 IPv6 設定，在持續推廣後108年已經有12間完成設定。

IPv4流量

IPv6流量

網路管理

網路連線、網管策略及具體辦理事項

➢ **108年度網路管理維運具體辦理事項**

6. 持續提供 cacti 可回溯的流量紀錄與查詢。

Tanet 100G骨幹(其他詳細資料)

IPv4統計資料

IPv6統計資料

國中小&實驗單位

均頭國中(統計資料)

台大竹山實驗林(統計資料)

網路管理

網路連線、網管策略及具體辦理事項

- **109年度網路管理維運具體辦理事項**

1. 預定更換 SIP Server
2. 持續推廣IPv6
3. 持續執行108年度項目

資安服務

資安服務、資安政策及具體辦理事項

- **108年度資安服務維運具體辦理事項**

1. 推動 ISMS 資訊管理系統
2. 舉辦連線單位管理委員會
3. 提供連線單位技術協助及各事項反應及聯絡窗口
4. 計畫經費控管及承接計畫相關行政流程
5. 配合教育部進行資安通報演練、社交工程演練、業務持續作業演練計畫
6. 其他教育部臨時交辦事項
7. 舉辦資安教育訓練

資安服務

資安服務、資安政策及具體辦理事項

➢ **108年度資安服務維運具體辦理事項**

8. 機房環境監測及電力設備維護

去年更換 ATS 系統後，至今約停電4次，除第一次停電須人工操作剩餘3次接自動切換完成。

環境監測即時狀態

2019-11-11 14:19:43

主機房現在機房溫度**20.8**度(C)
現在骨幹區溫度**23.37**度(C)
15K冷氣狀態-正常運作
20K冷氣狀態-正常運作

110V供電狀態-正常
75KV USP狀態-正常
75KV USP電池狀態-正電壓-正常
75KV USP電池狀態-負電壓-正常
目前機房供電狀況-**台電側供電，供電正常**

人院機房供電狀態-正常
人院現在機房溫度**24.64**度(C)

外氣運轉狀態-停止運轉

資安服務

資安服務、資安政策及具體辦理事項

- **108年度資安服務維運具體辦理事項**

9. 資安通報之通報、應變、審核及資安事件資料收集及分析。

	Time	Source	Protocol	Destination
1	2019-09-19 12:11:20.256539	[redacted]	HTTP	31.11.32.95
2	2019-09-19 12:11:29.689034	[redacted]	HTTP	188.121.43.14
3	2019-09-19 12:11:31.244026	[redacted]	HTTP	81.176.226.68
4	2019-09-19 12:11:38.150339	[redacted]	HTTP	213.174.157.134
5	2019-09-19 12:12:17.038611	[redacted]	HTTP	31.11.32.231
6	2019-09-19 12:47:20.665032	[redacted]	HTTP	136.243.133.242
7	2019-09-19 12:47:21.516406	[redacted]	HTTP	157.7.107.111
8	2019-09-19 12:47:23.822906	[redacted]	HTTP	46.182.5.20
9	2019-09-19 12:47:26.871571	[redacted]	HTTP	37.60.254.49
10	2019-09-19 12:47:30.076334	[redacted]	HTTP	64.71.38.206
11	2019-09-19 12:47:32.734339	[redacted]	HTTP	91.216.107.154

某國小於8~9月一直收到同一資安通報，經查為對外 WordPress 攻擊

資安服務

資安服務、資安政策及具體辦理事項

➢ **108年度資安服務維運具體辦理事項**

10. 骨幹網路監測及故障排除

10/23 19:00 ~ 23:00 亞太電信 A11 光纜遷移改接

10/23 22:00 連到台南主節點電路異常

台南主節點10點後斷線

台中主節點狀況

7點開始約到9點結束,9點後線路調整多次斷線，每次約1~5分鐘

資安服務

資安服務、資安政策及具體辦理事項

- **108年度資安服務維運具體辦理事項**

11. 阻擋 DDoS 攻擊，降低 DDoS 對網路服務的影響

10/22~11/7日南投區網遭受 DDoS 攻擊，連外網路不受影響

南投區網遭受攻擊時 session 約為3,000,000以上

網路效能系統11/1 14:40~15:10 100% -> 99.93%

資安服務

資安服務、資安政策及具體辦理事項

- **109年度資安服務維運具體辦理事項**

1. 舉辦資訊安全線上教育訓練
2. 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
3. 持續執行108年度項目

在管理委員會中有討論到資安法各級單位需完成事項，其中C、D級規範中皆有「一般使用者每人每年接受3小時以上之資通安全通識教育訓練」，連線單位表示，公務人員及教師有平台可以進行線上課程，但是其實單位中還有很多其他身份的人員，也有需要進行資通安全通識教育訓練，是否可以提供線上課程及測驗給各單位。

特色服務

推動特色、辦理成效與未來營運計劃

- **108年度服務特色辦理成效**

1. 協助連線單位資安通報查修
2. 協助遠距課輔硬體維護，及維持網路品質
3. IPv6 推廣

特色服務

推動特色、辦理成效與未來營運計劃

- **109年度創新服務目標與構想**
  1. 舉辦資訊安全線上教育訓練講座。
  2. 持續訂定網路查修相關文件，幫助連線單位查修效率。
  3. 資安法推動
  4. 協助連線單位 eduroam 建置
  5. 持續推動IPv6

特色服務

推動特色、辦理成效與未來營運計劃

- **109年度創新服務目標與構想**

6. 未來ASOC IPS架構。
   區網流量尖峰時會超過4G，超過兩台Sourcefire處理上限，故無法inline，目前使用mirror方式使用，未來透過分流設備濾掉加密與IPv6流量後，尖峰流量低於2.5G內即可inline使用。

特色服務

推動特色、辦理成效與未來營運計劃

➢ **109年度創新服務目標與構想**

6. 未來ASOC IPS架構。

特色服務

推動特色、辦理成效與未來營運計劃

- **109年度創新服務目標與構想**

7. Google M-LAB服務
   測速網頁 https://speed.measurementlab.net/#/

特色服務

推動特色、辦理成效與未來營運計劃

➢ **109年度創新服務目標與構想**

7. Google M-LAB服務
   11/20/2018 - 11/20/2019統計資料
   https://viz.measurementlab.net

灰色：台灣平均值　　棕色：TANet

特色服務

推動特色、辦理成效與未來營運計劃

- **109年度創新服務目標與構想**

  8. 機房節能，機櫃集中施行冷熱通道。

  - 南投區網中心機房目前空調運作
    - 夏季模式

      利用導風管及檔板將空調平均分散於機房

      可節省一台冷氣機的基本送風運轉
    - 冬季模式

      當外氣低於19度時啟動外氣引入

      可節省冷氣機用電

特色服務

推動特色、辦理成效與未來營運計劃

冷氣開啟利用導風管導風

引入外氣

特色服務

推動特色、辦理成效與未來營運計劃

- **109年度創新服務目標與構想**

  8. 機房節能，機櫃集中施行冷熱通道。

  - 109年度機房精進改善規劃
    - 重新計算機房使用狀況

      各機櫃空間使用U數

      各機櫃使用電力
    - 朝向模組化及最小化規劃

      模組化機櫃電力、空調、消防、外氣引入

      冷熱通道隔離

特色服務

推動特色、辦理成效與未來營運計劃

成效精進情形

執行成效評量改進意見項目成效精進情形

- 1.建立故障、資安技術問題集，供使用學校查詢，可節省區網人員回覆問題的工作量。

  目前執行情形：已於區網網頁呈現簡單網路查修相關資訊。

- 2.特別針對高中職資訊人員與縣網所轄國中小進行每年教育訓練，或以影音教材方式訓練。

  目前執行情形：教育訓練多為電腦實作課程，故以影音教材方式呈現有困難度，但是課程簡報皆會放到區網網頁-研討會資訊中。

- 3.建議移植其他區網中心開發之網路管理 如網路 delay 、 loss 等。

  目前執行情形：目前本中心使用套裝軟體 What‘s UP 監控區域網路連外及連線單位網路狀態。

成效精進情形

執行成效評量改進意見項目成效精進情形

- 4.建議與縣網合作之間訂定 MOU 。

  目前執行情形：已於管委會提出，但目前並未訂定。

- 5.利用遠端工具進行遠距客服服務。

  目前執行情形：部分情況可以遠端處理，如遇設備實體或網路拓樸問題還是需要到現場處理。

- 6.對區網中心維運計畫之網管及資安相關專案人員，建議應呈現其對應區網業務之績效，俾利後續能展現經費在此面上的運用效益。

  目前執行情形：依評審要求會盡量呈現工作績效。

成效精進情形

執行成效評量改進意見項目成效精進情形

- 7.對連線學校的服務是否有更積極更有系統的作法？區網縣網之間合作的方式能否不只是有事呼救而能予以制度化，並建立相關 SOP 。

  目前執行情形：以於管委會提出討論，目前尚未訂定。

- 8.管理委員會已於 2 月辦理一次，預計 12 月再辦理，兩者間隔太久，建議落實每半年至少辦理一次之原則。

  目前執行情形：本年度管委會召開次數不足，此項將放在未來改善重點項目。

  許多訊息以線上軟體 LINE 即時通知及溝通，未來將管理委員會與教育訓練舉辦在同一日，希望降低連線單位老師出席的不便，提高其出席率及會議效率。

  目前預計於109年度3月及10月各舉辦1場管理委員會及教育訓練，議題將為資安法推動、IPv6推廣、eduroam建置。

成效精進情形

執行成效評量改進意見項目成效精進情形

- 9.建議可參考其他區網提供之優質服務，逐年規劃引進導入來強化服務。

  目前執行情形：本年度5月份有至宜蘭區網中心參訪，得到許多寶貴意見，包含校園網路架構、防火牆設備及設定、機房自動滅火設備、區網維運經驗分享等等..

- 10.建議每年皆進行連線單位及教育訓練之滿意度調查等，以了解提供服務之績效。

  目前執行情形：本年度依評委意見，有進行滿意度調查，其成果將在以下簡報內呈現。

108年度區網中心

滿意度調查結果

採不記名調查，回收問卷15份

回收問卷單位分佈

整體網路連線是否順暢？

針對區網人員協助處理資安通報事件滿意度為何？

針對區網人員聯繫協調與相關資訊取得的滿意度為何？

針對區網人員熱忱及親和力的滿意度滿意度為何？

回收問卷-家電信業者(ISP)分佈

請問您對電信業者(ISP) 服務滿意度為何？

請問您對電信業者(ISP) 維修速度滿意度為何？

有參加教育訓練者填寫

請問對區網舉辦的教育訓練整體滿意度為何？

有參加教育訓練者填寫

請問對本次教育訓練講師滿意度為何？

有參加教育訓練者填寫

請問對本次教育訓練對於網管業務是否有幫助？

簡報結束
謝謝