108 年度區域網路中心年終成果基礎資料彙整表

臺北區域Ⅰ網路中心

（負責學校：國立台灣大學）

108 年 11 月 08 日

目 錄

壹、基礎維運資料

一、經費及人力

請依下列項目提供本年度報告資料

1. 網路中心經費使用	(1) 核定計畫金額：1,720,000 (2) 教育部補助金額：1,720,000 (3) 自籌金額：0 (4) 實際累計執行數（至 11 月）：1,314,090
2. 網路中心人力數	(1).專任：2 人 (2).兼任：0 人 （請填數字）。 其中包含教育部補助： (1).網管人員：1 人，證照數：3 張。 (2).資安人員：1 人，證照數：1 張。

二、 請詳述經費使用情形及績效檢討。

說明:1.請填寫前 3 年度(105-107)經費使用達成率及本(108)年度預計達成率。
2.檢討歷年度達成率。(如有經費繳回，請述明原因)

年度	教育部核定	實支總額	人事費繳回	達成率	扣除繳回達成率
105	1,579,088	1,367,903	87,140 (8、9 月)	86.67%	91.7%
106	1,580,000	1,309,762	261,420 (1 至 6 月)	82.90%	99.33%
107	1,720,000	1,577,987	51,040 (8 月)	91.74%	95%

108	**1,720,000**	1,314,090 (11 月)	0	97% (預估)	97% (預估)

三、 請詳述本部補助貴區網中心網管及資安人力之服務績效。

說明:1.請填寫前 3 年度(105-107)人員任務配置及異動情形，及本(108)年度人員配置運作情形。
2.檢討歷年度人員異動因素。(如有人事經費繳回，請述明原因)

網管人員人力規劃:

1.臺北區網網路中心 I 網路管理維運。

2.網路服務品質分析與監控。

3.區網雲端租賃服務管理維運。

4.連線單位網路故障與排除。

資安人員人力規劃:

1.資安事件通報與處理。

2.資安事件鑑識與調查。

3.DDoS 異常通報與回覆

4.網路異常分析與監控。

因 105~107 年因聘僱不到資安人員導致達成率偏低。

108 年度資安與網管人員 1~12 月皆滿聘，已無此現象。

四、 基礎資料(網管及資安)

請依下列項目提供本年度報告資料

(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	31	14	1	5	52
	連線比例		2%	61%	27%	2%	10%	單位(校)數 / 總計
(2)連線頻寬 (以電路數統計)	專線(非光纖)							
	光纖	10M(不含)以下						
		10M(含)以上 100M(不含)以下						
		100M(含)以上 500M(不含)以下						
		500M(含)以上 1G(不含)以下						
		1G(含)以上 10G(不含)以下		28	14	1	5	
		10G(含)以上	1	3				
	其他(如 ADSL 等)							
	連線電路小計							

	縣(市)教育網路中心		連線頻寬(1)	連線頻寬(2)	備註
(3)連線縣(市)教育網路中心	1.	臺北市	Ipv4:10G	Ipv6:1G*2	
	2.				
	3.				

	單位名稱		連線頻寬(1)	連線頻寬(2)	備註
(4)非學校連線單位(不含 ISP)	1.	新北市立圖書館	1G		
	2.	中華民國高級中等學校體育總會	1G		
	3.	財團法人大學入學考試中心	1G		
	4.	中華民國學生棒球運動聯盟	1G		
	5.	國家地震中心	1G		

(5)連線 TANet	臺灣學術網路(TANet)	連線臺北主節點	連線新竹主節點	
		頻寬 100 Gbps	頻寬 100 Gbps	

	ISP 名稱(AS)		連線頻寬(1)	連線頻寬(2)	備註
(6)ISP 線路	1.	中華電信 Hinet(AS3456)	3G		

	2.	新世紀資通 Seednet(AS4780)	2G		
	3.	新世紀資通 NCIC(AS9919)			
	4.	中嘉和網 KBT(AS9461)	1G		
	5.	台灣固網 TFN(AS9964)	1G		
	6.	亞太電信 APG(AS17709)	1G		
	7.				
	8.				
	9.				
(7)補充說明：					
(8)連線資訊	請依附表「學校/單位連線資訊詳細表」格式填附				

(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. 1、2 級資安事件處理： (1) 通報平均時數： 0.586 小時。 (2) 應變處理平均時數： 0.017 小時。 (3) 事件處理平均時數： 0.602 小時。 (4) 通報完成率： 99.969% 。 (5) 事件完成率： 99.627% 。 2. 3、4 級資安事件通報： (1) 通報平均時數： 0 小時。 (2) 應變處理平均時數： 0 小時。 (3) 事件處理平均時數： 0 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： 0.206 小時。
(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： 81.633% %。 (由教育部參照資安通報演練作業現況提供) 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? V 是 □否 (2)是否符合稽核要求? V 是 □否 (3)符合資安專業證照人數： 2 員 (4)維護之主要網站進行安全弱點檢測比率： 100 %。

貳、請詳述貴區網中心之網路連線、網管策略及具體辦理事項(網路管理)

說明:1.108 年度網路管理維運具體辦理事項。
2.109 年度網路管理營運方針。

108 年度網路管理維運具體辦理事項:

1. Cacti 結合 Line Notify 群組通知

✱不需架設 Line BOT Server

✱不需監控 Email Server 及 Parse 內容

✱僅需四行程式

✱維護簡單且更即時

2. 網路設備設定檔自動備份

✱支援使用 Telnet or SSH 連線設備

✱每週自動備份設定檔

✱支援: Cisco、Gigamon、FotiGate

3. 連線單位技術支援

資安設備阻擋封包分析:因 WAF 規則有誤，導致圖書館日治時期統計資料庫無法正常連線。

4. TANet 2019 論文發表

以校園網路連線大數據驗證六度分隔理論：

以六度分隔理論所描述之現象，提出不同的驗證方法，並運用大數據資

料統計校園網路連線資訊，包括 IP 路由節點數與 BGP AS-Path 長度，來驗證六度分隔理論之正確性。

109 年度網路管理營運方針

1. DNS Log 分析

資安事件中常出現因使用者查詢惡意 Domain Name 導致校內 DNS Server 觸發資安事件，但從 DNS Server 若開啟詳細 Log 可能影響 DNS 正常運作，且 Log 也無法詳實記錄 Quest and Reply 之詳細結果。

DNS 封包傳輸方式為明碼未加密，因此若能從封包中擷取出 DNS Quest and Reply 之詳細結果將有助於資安事件之調查。

2. Layer2 封包分析

校園網路中 Edge 端最常影響使用者網路體驗，就是 Layer2 同網段中有太多異常封包，例如: Broadcast、Multicast 及 Unicast Flooding，預計開發可辨識 Layer2 封包中異常之網路流量。

參、請詳述貴區網中心之資安服務、資安政策及具體辦理事項(資安服務)

說明:1.108 年度資安服務維運具體辦理事項。
2.109 年度資安服務目標(實施措施)。

108 年度資安服務維運具體辦理事項:

1. 資安事件

	106	107	108
1、2 級資安事件處理			
通報平均時數	2.70 小時	1.343 小時	0.586 小時
應變處理平均時數	0.05 小時	0.026 小時	0.017 小時
事件處理平均時數	2.76 小時	1.369 小時	0.602 小時
通報完成率	98.90%	99.86%	99.969%
事件完成率	99.91%	99.92%	99.627%
3、4 級資安事件通報	無	無	無
資安事件通報審核平均時	0.60 小時	0.519 小時	0.206 小時
資料更新完整校數	72.92%	73.47%	81.633%

108 年度資安通報平均時數 0.586 小時，事件處理平均時數 0.602 小時，已經縮短至 1 個小時內，資訊完整度也進步至 81.633%。

2.推廣 Let ‘s Encrypt 免費憑證之使用:

Let ‘s Encrypt 由網際網路安全研究小組（縮寫 ISRG）提供服務。旨在以自動化流程消除手動建立和安裝憑證的複雜流程，並推廣使全球資訊網伺服器加密服務，為安全網站提供免費的 SSL/TLS 憑證。主要贊助商包括電子前哨基金會、Mozilla 基金會、Akamai 以及思科。因此提供之憑證確實可靠且具安全性。

3.DDoS 通報機制改善

目前北區 A-SOC 已有自動偵測與 email 通知機制，可主動告知被攻擊之區網連線單位，及攻擊之來源與目的等相關資訊，並詢問是否進行封包清洗作業。

4.設立技術文件專區

在區網網站新設立技術文件專區 http://www.tplrc.edu.tw/el.php，將逐步整理相關資安及網路技術文件，可供網管人員參考與自行學習。

109 年度資安服務目標

1.網路異常偵測與阻擋系統

- ✱ 現況: Threshold based 接近頻寬滿載時才啟動
- ✱ 未來: 分佈比例異常即啟動
- ✱ 適用於 Out of Band 之網路架構
- ✱ 可偵測 Port Scan & DDoS 等網路異常流量

肆、請說明貴區網中心服務推動特色、辦理成效與未來營運計劃(特色服務)

說明:1.108 年度服務特色辦理成效。
2.109 年度創新服務目標與構想。

108 年度服務特色辦理成效:

1. TCP-based 網路品質監控

使用 nProbe 可觀察 Latency 及網路封包異常遺失等行為，目前已佈建完成，可 24 Hr 監控臺大邊界路由器所有對外網路連線情況，具體成果也受邀於 TANet100G 研討會花蓮場發表。

2. Line Bot based 即時網路資訊情搜與通報

- ✱ Ptt.cc 論壇校園版爬文
- ✱ 校內或 TANet 網段出現在攻擊/被攻擊 網站中
- ✱ Talos 黑名單搜尋
- ✱ CVE 搜尋 Cisco、Windows、Apache 等常用系統

109 年度創新服務目標與構想：

1. Line Bot 自動語意分析系統:

可用口語化之方式詢問網路狀況，Line Bot 可自動搜尋相關資訊後呈現於 Line 群組訊息中。

伍、前(各)年度執行成效評量改進意見項目成效精進情形

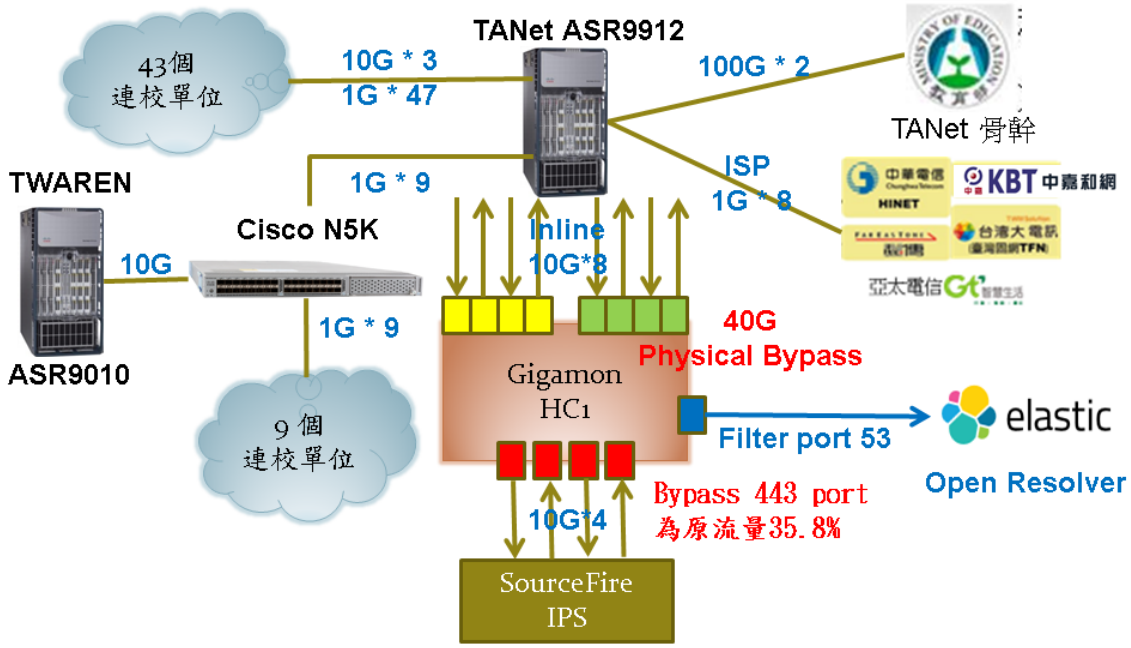
委員建議	回覆
1. TCP Based 網路品質監控僅在台大校園網路，並位於區網建置，建請移至區網建置時，同時建立 SOP ，以考慮移植至其他區網和學校。同時評估以 OPEN DATA 方式呈現。	因區網骨幹尖峰流量進出加總超過 25 Gbps 流量，已經超過一般市面上可購得 PCI-E based 網卡 10Gbps 之處理能力，因此暫時無法將監控系統移植於區網網路進行監控。目前預計將此技術舉辦相關技術研討會，請有興趣建置之連線單位可自行建置 TCP Based 網路品質監控系統。
2.考慮服務學校與區網配合，制定 DDOS 攻擊處理程序 SOP ，以縮短處理時間，更有效率解決問題。	目前北區 A-SOC 已有自動偵測與 email 通知機制，可主動告知被攻擊之區網連線單位，及攻擊之來源與目的等相關資訊，並詢問是否進行封包清洗作業。
3.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	在區網網站新設立技術文件專區 http://www.tplrc.edu.tw/el.php，將逐步

的工作量。	整理相關資安及網路技術文件，可供網管人員參考與自行學習。
4.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。	依委員建議已經回覆於”108 年度區域網路中心年終成果基礎資料彙整表”中第三項、請詳述本部補助貴區網中心網管及資安人力之服務績效。
5.對區網之網路流量由去年的 9.9G 成長至 21G 建議對應的網管及資安服務機制應有相關配套調整規劃。	Cacti Threshold 及 Syslog 異常偵測加上 Line Notify 自動通知功能，可加速處理效率。
	使用”即時網路資訊情搜與通報”並結合 Line 自動通知功能，可快速處理及應映各種網路異常情況。
6.對區網中心所提供連線服務學校之 DDOS 清洗服務 建議依實際運作對照教育部所訂定之處理 SOP 提出相關修正建議以利各校能更有效率的因應 DDOS 資安事件的處置。	目前北區 A-SOC 已有自動偵測與 email 通知機制，可主動告知被攻擊之區網連線單位，及攻擊之來源與目的等相關資訊，並詢問是否進行封包清洗作業。
7.對評估建議連線學校採用之免費憑證請瞭解其安全性。	Let‘s Encrypt 由網際網路安全研究小組(縮寫 ISRG)提供服務。旨在以自動化流程消除

	手動建立和安裝憑證的複雜流程，並推廣使全球資訊網伺服器加密服務，為安全網站提供免費的 SSL/TLS 憑證。主要贊助商包括電子前哨基金會、Mozilla 基金會、Akamai 以及思科。因此提供之憑證確實可靠且具安全性。
8.對資安事件的通報處理效率應思考如何精進。	108 年度資安通報平均時數 0.586 小時，事件處理平均時數 0.602 小時，已經縮短至 1 個小時內，相較去年有大幅進度。
9.建議爾後簡報資料請同步更新至網站以利委員審查。	今年若簡報有更改，將同步更新於區網網站與教育部 TANet NOC 網站。
10.資安通報平均通報時數及事件處理平均時數已較去年進步，但建議仍需持續努力，逐步縮短至 1 個小時內。另外聯絡資訊之資訊完整度：73.47%亦可再加強。	108 年度資安通報平均時數 0.586 小時，事件處理平均時數 0.602 小時，已經縮短至 1 個小時內，資訊完整度也進步至 81.633%。

附表 1：區網網路架構圖

一、 區網與連線單位(含縣(市)教育網路、連線學校、其他連線單位等)、TANet、Internet(Peering)的總體架構圖



二、網路配合各種應用架構(如連線分流、頻寬管理)或資安架構(防火牆、IDS/IPS/WAF)的規劃或實際運作架構

同上圖

附表 2：連線資訊詳細表

		單位/學校名稱	電路頻寬	電路服務商	備註
縣(市)教育網中心	1.	臺北市	10G	亞太	
	2.	臺北市	2G	中華	
	3.				
	4.				
	5.				
大專校院	1.	國防大學（復興崗校區）	1G	中華	
	2.	國防醫學院	1G	台灣固網	
	3.	國立臺灣大學	10G	Dark Fiber	
	4.	國立臺灣大學醫學院附設醫院	1G	中華	
	5.	國立臺灣師範大學(公館校區)	2G	中華	
	6.	國立空中大學	1G	中華	
	7.	國立臺北護理健康大學	1G	中華	
	8.	國立臺灣藝術大學	1G	亞太	
	9.	國立臺灣藝術大學	1G	中華	
	10.	國立臺北藝術大學	1G	中華	
	11.	國立臺北商業大學	1G	中華	
	12.	銘傳大學	1G	中華	
	13.	實踐大學	1G	中華	
	14.	臺北醫學大學	1G	台灣固網	
	15.	真理大學台北校區	1G	台灣固網	
	16.	大同大學	1G	遠傳電信	
	17.	龍華科技大學	1G	中華	
	18.	宏國德霖科技大學	1G	中華	
	19.	亞東技術學院	2G	遠傳電信	
	20.	致理科技大學	1G	中華	
	21.	黎明技術學院	1G	中華	
	22.	康寧大學	1G	中華	
	23.	華夏科技大學	1G	中華	
	24.	私立明志科技大學	1G	遠傳電信	
	25.	臺北海洋技術學院	2G	遠傳電信	
	26.	德明財經科技大學	1G	中華	
	27.	法鼓文理學院	1G	中華	
	28.	臺北市立大學	1G	臺灣智慧光網	
	29.	國防部軍事情報局軍事情報學校	1G	亞太	

	30.	臺北科技大學	10G	中華	
	31.	臺北基督學院	1G	台灣固網	
	32.	臺灣科技大學	10G	Dark Fiber	
	33.				
	34.				
	35.				
高中職校	1.	國立臺灣師範大學附屬高級中學	1G	亞太	
	2.	臺北市私立育達高級商業家事職業學校	1G	中華	
	3.	臺北市私立協和祐德高中	1G	臺灣智慧光網	
	4.	臺北市私立文德女子高級中學	1G	中華	
	5.	臺北市私立復興實驗高級中學	1G	臺灣智慧光網	
	6.	臺北市私立開平餐飲職業學校	1G	中華	
	7.	桃園縣光啟高級中學	1G	中華	
	8.	新北市南山高級中學	1G	中華	
	9.	新北市私立徐匯高級中學	1G	中華	
	10.	新北市清傳高級商業職業學校	1G	中華	
	11.	新北市東海高級中學	1G	中華	
	12.	新北市私立樹人高級家事商業職業學校	1G	中華	
	13.	新北市能仁高級家事商業職業學校	1G	中華	
	14.	大同高中	1G	中華	
國中小學	1.	國立臺北教育大學附設實驗國民小學	1G	臺灣智慧光網	
	2.				
	3.				
	4.				
	5.				
非學校連線單位	1.	新北市立圖書館	1G	中華	
	2.	中華民國高級中等學校體育總會	1G	中華	
	3.	財團法人大學入學考試中心	1G	Dark Fiber	
	4.	中華民國學生棒球運動聯盟	1G	台灣固網	
	5.	國家地震中心	1G	Dark Fiber	

※備註: 1.請以電路為單位填寫，若學校有多條連線，請個別填寫多列。

2.表格可自行調整。