

# 106 年度區域網路中心年終成果基礎資料彙整表

## 桃園 區域網路中心(負責學校：國立中央大學)

### 一、基礎維運資料：

(一)、報告事項(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： <u>3,670,000</u> (2) 教育部補助金額： <u>2,410,000</u> (3) 自籌金額： <u>1,260,000</u> (4) 實際累計執行數(至11月)： <u>77.66</u> %
2. 網路中心人力數	(1). 專任： <u>3</u> 人 (2). 兼任： <u>4</u> 人 (請填數字)。 其中包含教育部補助： (1). 網管人員： <u>2</u> 人，證照數： <u>2</u> 張。 (2). 資安人員： <u>1</u> 人，證照數： <u>2</u> 張。

(二)、基礎資料(網管及資安)：請依下列項目提供本年度報告資料

### 1. 區網中心連線資訊彙整表：

	項目	縣(市)教育網路中心	大專院校	高中職校	其他學校	其他單位	總計	
(1)連線數 (以單位(校)數統計)	單位(校)數	3	14	27		8	52	
	連線比例						註：單位(校)數 / 總計	
(2)連線頻寬 (以電路數統計)	專線			1			1	
	光纖	10M(不含)以下						
		10M(含)以上 100M(不含)以下			6			6
		100M(含)以上 1G(不含)以下		12	19		8	39
		1G(含)以上 10G(不含)以下		2				2
		10G(含)以上						
		其他(如 ADSL 等)			1			1
	連線電路小計							
(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.	桃園市網	10G(亞太電信)			2G(中華電信)		ipv4-10G ipv6-2G
	2.	連江縣網	1G					
	3.	金門縣網	1G					
(4)連線其他單位	其他單位名稱		連線頻寬(1)			連線頻寬(2)		備註

(非 ISP)	1.				
	2.				
	3.				
	4.				
	5.				
(5)連線 TANet 及其他 ISP 線路	臺灣學術網路(TANet)		連線 <u>台北</u> 主節點	連線 <u>新竹</u> 主節點	
	(1)		頻寬 <u>40</u> Gbps	頻寬 <u>40</u> Gbps	
	其他 ISP		連線頻寬(1)	連線頻寬(2)	備註
	1.	HINET	2G		
	2.	SeedNet	1G		
	3.	亞太線上	100M		
	4.	和信	1G		
5.	速博	1G			
6.	台固	1G			
(6)補充說明：					
(7)連線資訊	請依附表「學校/單位連線資訊詳細表」格式填附				

## 2. 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. <u>1、2級資安事件處理：</u> (1)通報平均時數： <u>2.97</u> 小時。 (2)應變處理平均時數： <u>0.37</u> 小時。 (3)事件處理平均時數： <u>3.34</u> 小時。 (4)通報完成率： <u>96.59%</u> 。 (5)事件完成率： <u>98.98%</u> 。
	2. <u>3、4級資安事件通報：</u> (1)通報平均時數： <u>無</u> 小時。 (2)應變處理平均時數： <u>無</u> 小時。 (3)事件處理平均時數： <u>無</u> 小時。 (4)通報完成率： <u>無</u> 。 (5)事件完成率： <u>無</u> 。 資安事件通報審核平均時數： <u>0.28</u> 小時。

<p>(2)網路中心配合本部資安政策。</p>	<ol style="list-style-type: none"> <li>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：<u>90.48</u> %。 (由教育部參照資安通報演練作業現況提供)</li> <li>區網網路中心依資通安全應執行事項： <ol style="list-style-type: none"> <li>是否符合防護縱深要求？<input checked="" type="checkbox"/>是 <input type="checkbox"/>否</li> <li>是否符合稽核要求？<input checked="" type="checkbox"/>是 <input type="checkbox"/>否</li> <li>符合資安專業證照人數：<u>22</u> 員</li> <li>維護之主要網站進行安全弱點檢測比率：<u>100</u> %。</li> </ol> </li> </ol>
-------------------------	---

### (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。

#### 1. 網管人力：

維護區網網路正常連線：線路異常排除，通訊網路設備管理，建置網路管理系統，dns 及 www 管理，機房及基礎環境(電力，空調，溫濕度，消防設備)維護，辦理網路管理技術研討會，臨時交辦事項。

#### 2. 資安人力：

資安通報審核及演練，資安事件處理，社交演練，異常流量 ip 偵測及處理，協助 iso27001 資安認證，弱點掃描及追蹤處理，個資保護系統維護，辦理資安研討會，臨時交辦事項。

### 二、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)。

1. 區網對外透過 paloalto 5060 進行 p2p 管制，有效降低智財侵權事件。

<http://www.tyrc.edu.tw/index.php/PaloAlto5060>

2. 即時流量監控，掌控流量變化

<http://www.tyrc.edu.tw/index.php/MRTG> 。

3. 計算流量 Top N 系統，監控大流量 ip

[http://www.tyrc.edu.tw/index.php/TOP\\_N](http://www.tyrc.edu.tw/index.php/TOP_N) 。

4. 建置 GGC 加速 google 網站的服務。

5. 計算桃園區網 網路應用分布圖，監控各種網路應用的變化。

6. 協助連線單位啟動 ipv6 連線 <http://www.tyrc.edu.tw/index.php/IPv6>

及監控 ipv6 mrtg 流量變化 <http://140.115.2.26/tutorial/ipv6Mrtg.action>

### 三、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)。

1. 桃園區網中心(中央大學)已連續九年取得 ISO27001 認證，今年 3/22 拿到 ISO 27001 改版證書並依規定接受複查以保持證照有效性，提供本大學資訊技術及台灣學術網路桃園區域網路中心相關之服務。

2. 啟動 paloalto 5060 IPS 功能，制定 policy 進行 Vulnerability Protection, Anti spyware, URL filtering 保護有效降低網路攻擊事件。

3. 建置 Spark 異常流量偵測系統，偵測異常流量，即時解決網路異常。

<http://www.tyrc.edu.tw/index.php/Spark>

4. 加入北區學術網路 SOC(台大)計畫，提供資安防護與資訊分享機制，監控網路異常 ip。

<http://www.tyrc.edu.tw/index.php/ASOC>

5. 辦理資安及網路管理教育訓練及研討會。

<http://www.tyrc.edu.tw/index.php/Training>

6. 新版教育體系資通安全暨個人資料管理規範上路，中央大學以學務處為代表，105 年 12 月率先通過驗證，成為國內首批通過教育體系個人資料管理規範驗證學校之一。目前全校共有 22 個一級單位擔任推動窗口，並已完成 72 個一、二級單位導入 BS 10012 個人資料管理系統 (PIMS)。

<http://www.ncu.edu.tw/campus/article/1968>、<https://pims.ncu.edu.tw/>

#### 四、請說明貴區網中心服務推動特色、辦理成效與未來運營計劃(特色服務)。

##### (一)、服務推動特色

###### 1. 以網路分流器彈性部署入侵偵測與防禦系統

透過以網路分流器，彈性部署入侵偵測與防禦系統，將區網中主要需保護的網段流量導入 IPS 防禦系統，減輕 IPS 系統的負荷，使得原有 IPS 可以持續運作。也應用網路分流器的可視性及彈性設定，將處理重要資料的行政單位網段流量導入 Security Onion 開源入侵偵測系統平台，作為進一步詳細偵測可疑的網路行為。

###### 系統優點：

- (1)對於高速之 100G 網路頻寬透過網路分流器設定特定服務做資安防護，除有效降低資安設備的等級，並可提供 1:1 之 Netflow 資料供後端 Spark 網路流量偵測系統分析網路異常流量。
- (2)透過網路分流器分流過濾功能，非關鍵業務網段不通過入侵防禦系統，可以使原有之入侵防禦系統仍可繼續使用。
- (3)彈性之網路架構及設定，可依需求彈性切換網路分流模式，提升資安設備運作成效。

###### 2. 雲端 Spark 異常流量偵測系統

以處理巨量資料速度更快的 Spark 架構結合原 FDNS 系統之 Hadoop 架構，彌補 Hadoop MapReduce 的緩慢，系統可於監測大量的網路流量中篩選出異常的流量及可疑主機，並將資料寫入 Mongo 資料庫，提供網管工作人員透過 web 介面查詢每十分鐘、每小時、每天之異常之網路流量及可疑主機排行。系統並已推廣至花蓮區網及高屏澎區網使用。

###### 系統優點如下：

- (1)使用 Spark 協同 Hadoop 架構偵測網路異常流量的平台。
- (2)Spark 模組負責即時的運算，可以充分利用 Spark in-memory computing 特性，在大量的 NetFlow Data 中快速篩選出異常網路行為的主機。Hadoop 模組則處理大量批次作業，以每小時進行大量資料分析作業。

###### 3. GGC

桃園區網於 2015 年 3 月 9 日正式啟用 Google Global Cache(GGC)服務，這項服務使用者不需變更任何網路設定，就可以更有效率的使用 google 網路內容服務。系統包括三部 Dell R720 伺服器、144TB 的資料儲存空間及 10G 的網路介面連接到桃園區網中心 ASR9010。

###### 系統優點：

- (1)升對桃園區網各連線學校的服務品質。
- (2)減少桃園區網出口頻寬壅塞，使其他網路服務更加順暢。

###### 4. 教育雲北區雲端資料中心：

###### 提供的資源：

CPU: 216 vCPU (108 core), RAM: 1136 GB, HD: 可用 70TB (鏡像的備份)

###### 使用的軟體：

雲端管理軟體:VMware (2016/4/28 完成轉換)

虛擬化儲存軟體：(共契採購)

**教育雲上的服務系統：**

- 數學小學堂系統 ( 3vm)
- 中華開放教育平台 ( 11vm)
- 扶輪社偏鄉教學系統 (4 vm)
- 體育雲-全民運動資訊系統 (13 vm)
- 體育資訊雲端 ( 3vm)
- 教師研習平台 (2 vm)
- 臺灣微積分題庫 (1 vm)
- 教育體系單一帳號驗證授權平臺 (10 vm)

**(二)、未來運營計劃(特色服務)。**

1. 處理 106 連線單位的滿意度調查/意見回饋，辦理連線單位建議的教育訓練及研討會：資安技術、網路攻擊、流量控管、虛擬主機的資安管理、無線網路環境建置、網管工具類，IPv6 經驗分享、ISMS、PIMS。
2. 區網主幹轉送封包之監聽/分析/攻擊偵測，Spark 偵測系統更新版本及特色推動。
3. 教育部連網設備及頻寬升級後相關管理系統更新。
4. 加強雲端服務:提供建置私有雲及教育雲服務之經驗分享/推廣。
5. 強化基礎設施-發電機更新。
6. 協助區網連線單位加強頻寬及連線品質問題。

**五、前(各)年度執行成效評量改進意見項目成效精進情形。**

1. 桃園區域網路中心網域已更換為 tyrc.edu.tw，原 tyrc.ncu.edu.tw 已停止使用。
2. 網路流量監測機制均已透過 Cacti 反應即時流量於區網中心網頁，強化 ASR9010 Netflow Ver9 的收集及分析。
3. 輔導離島及經營教育雲的相關經驗，目前已放上桃園區網網站分享。
4. 今年於 11/18 至連江縣網辦理離島的研討會，日後將持續每年的離島的研討會，以加強和縣市網之間的交流與溝通。
5. 桃園區網於 7 月份進行 UPS 更新工程，更換成新的模組式 UPS，200K-A，200K-B，並增加切換二部發電機之開關，以避免單一發電機失效造成斷電，明年度並已提出購置更換新的發電機，以確保電力供應，避免網路服務中斷。
6. 桃園區網網站之公告除轉發訊息，其它發佈訊息，由承辦人撰擬後，需呈主管審視後始發佈公告，以免描述不精確造成誤解。

附表：連線資訊詳細表

		單位/學校名稱	電路類型	電路頻寬	電路服務商	備註
縣(市)教育網中心	1.	桃園市網	光纖	12G	中華電信 2G 亞太 10G	
	2.	連江縣網	光纖	1G	中華電信	
	3.	金門縣網	光纖	1G	中華電信	
	4.					
	5.					
大專院校	1.	中原大學	光纖	1G	台灣固網	
	2.	元智大學	光纖	1G	中華電信	
	3.	銘傳大學	光纖	1G	中華電信	
	4.	萬能大學	光纖	10G	中華電信	
	5.	開南大學	光纖	1G	中華電信	
	6.	中央大學	光纖	10G	中華電信	
	7.	國防大學	光纖	1G	中華電信	
	8.	中央警察大學	光纖	100M	中華電信	
	9.	健行科技大學	光纖	1G	中華電信	
	10.	體育大學	光纖	200M	中華電信	
	11.	陸軍專科學校	光纖	500M	中華電信	
	12.	南亞技術學院	光纖	1G	中華電信	
	13.	國立臺北商業大學(桃園校區)	光纖	200M	中華電信	
	14.	新生醫專	光纖	500M	中華電信	
高中職校	1.	楊梅高中	光纖	100M	中華電信	
	2.	桃園高中	光纖	100M	中華電信	
	3.	中壢高中	光纖	100M	中華電信	
	4.	成功工商	光纖	100M	中華電信	
	5.	治平高中	光纖	100M	中華電信	
	6.	復旦中學	光纖	100M	中華電信	
	7.	桃園農工	光纖	100M	中華電信	
	8.	育達高中	光纖	50M	中華電信	
	9.	振聲高中	光纖	100M	中華電信	
	10.	六和高中	光纖	100M	中華電信	
	11.	大華中學	光纖	100M	中華電信	
	12.	桃園啟智學校	光纖	100M	中華電信	
	13.	方曙中學	光纖	E1	中華電信	
	14.	大興高中	光纖	100M	中華電信	
	15.	龍潭高中	光纖	100M	中華電信	
	16.	內壢高中	光纖	50M	中華電信	
	17.	中壢家商	光纖	100M	中華電信	
	18.	新興高中	光纖	50M	中華電信	
	19.	永平工商	光纖	100M	中華電信	

	20.	至善高中	光纖	50M	中華電信	
	21.	中壢高商	光纖	100M	中華電信	
	22.	陽明高中	光纖	50M	中華電信	
	23.	啟英高中	光纖	100M	中華電信	
	24.	武陵中學	光纖	100M	中華電信	
	25.	清華高中	光纖	50M	中華電信	
	26.	桃園美國學校	光纖	1G	接開南大學	
	27.	漢英高中	提供 dns 註冊			
其他學校	1.					
	2.					
	3.					
	4.					
	5.					
其他單位 (非 ISP)	1.	核能研究所	光纖	100M	中華電信	
	2.	資策會教育訓練處	光纖	1G	接中央大學	
	3.					
	4.					
	5.					