



桃園區網中心 108年度年終執行成效報告

單 位：國立中央大學

報告人：許時準組長

Email：center20@ncu.edu.tw

電 話：03-4227151#57507

日 期：2019/11/21



報告大綱

1. 經費與人力
2. 維運與連線服務
3. 網路管理及資安服務
4. 特色服務
5. 107年度缺失改善與精進
6. 109年度預計推動之重點工作
7. 綜合建議

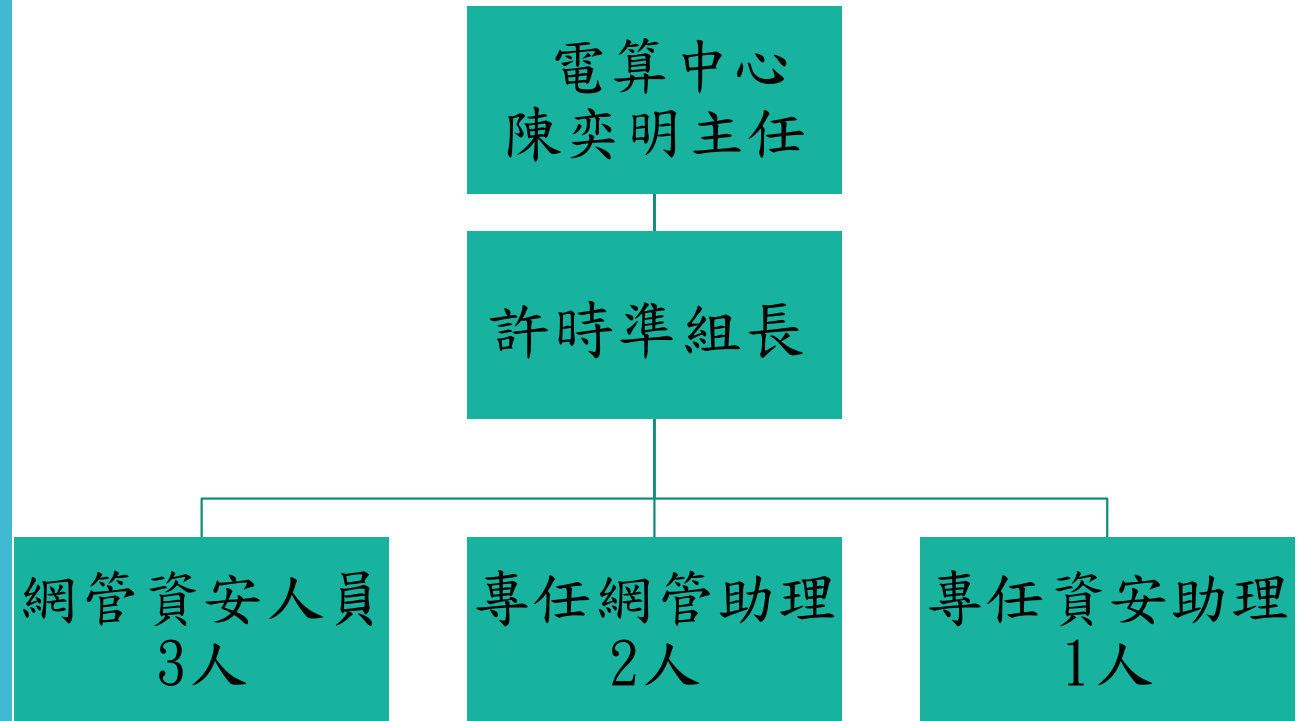


1.經費與人力





桃園區網 人力資源





桃園區網 經費統計

核定計畫金額	4,765,000
教育部補助金額	3,505,000
自籌金額	1,260,000
實際累計執行數 (至11月)	83%



105-108經費 使用達成率

年度	達成率	經費繳回原因
105年	97.01%	
106年	97.29%	
107年	93.76%	繳回73724元，因計畫經費預估人員取得碩士學歷薪資提升，但未能在預定時間畢業。
108年	預估99%	



專任網管 人員任務 與績效

網管人員(2位)的任務與績效

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 server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。

教育部北區教育雲端資料中心相關業務

協助連線單位處理雲端服務相關問題



專任資安 人員任務 與績效

資安人員(1位)的任務與績效

資安通報審核及演練，資安事件處理

異常流量IP偵測及處理

協助ISO27001資安認證, 個資保護系統維護

弱點掃描，網頁檢測及追蹤處理

辦理資安研討會，臨時交辦事項。



2 . 維運與連線服務



機房電力、 空調、溫溼 度

- ❑ 持續機房維運建設(電力、空調),維持良好網路運作
 - ❑ 除現有450KVA發電機組及配電線路外,本年度新增500KVA發電機組1座。
 - ❑ 模組式UPS, 200K-A, 200K-B, 並具備切換二部發電機之開關
 - ❑ 10噸x3+1台窗型冷氣空調系統
 - ❑ 網路溫/濕度計, 建置機房溫度/濕度監看網頁





建置桃園區 網中心網站 常見問題FAQ

- 以使用者為中心提供更友善的介面與服務，建立網管、資安技術問題集FAQ，供連線學校查詢，可提供連線學校老師先自行排除問題，並節省區網人員回覆問題的工作量。



桃園區域網路中心

[首頁](#) [關於桃園區網](#) [網路流量](#) [會議資料](#) [教育訓練](#) [資安服務](#) [FAQ](#)

目錄

- [1. 如何申請加入區網連線](#)
- [2. 網路不通](#)
- [3. 網路緩慢](#)
- [4. 部分網站無法到達](#)

如何申請加入區網連線

- Q 1：如何申請桃園區網連線？

A：

- 申請單位必須為各級學校或學術單位，並請貴校先向教育部資料司申請IP 及 Domain Name。
- 請貴校自行接洽ISP業者(中華電信、遠傳、亞太....等國內ISP)選擇適合的網路頻寬。
- 與桃園區網中心聯繫介接事宜。
週一至週五：8-17時 電話：03-4227151 (分機轉 57555/57566)
週一至週五：17-22時 電話：03-4227151 (分機轉 57511)

- Q 2：如何提升網路連線頻寬？

A：

- 申請單位請評估現有頻寬是否不敷使用？並先向桃園區網中心洽詢是否有足夠的網路連接埠可供提升後使用？
- 另外請洽詢各ISP 線路提升施工，例如中華電信可洽詢桃園營運處企業客戶科，其他ISP請逕洽各業者客服專線。
- 中華電信可撥打客服專線0800080123，提供學校的光纖號碼和學校的基本資料

網路不通

[網管類](#)

[資安類](#)

[其他](#)



桃園區網維運—機房管理

■ 訊息公告

■ 機房工作日誌

桃園區域網路中心

首頁 關於桃園區網 網路流量 會議資料 教育訓練 資安服務 舊站 >

桃園區域網路中心 Taoyuan Network Regional Center

區網網路流量

區網對外:	17.8%	7109.2 Mb/s
區網-連江:	17.4%	93.3 Mb/s
區網-金門:	43.3%	465.3 Mb/s
區網-桃園:	40.3%	5192.4 Mb/s

(每5分鐘更新一次)

上次更新時間: 2019-10-21 9:25 (星期一)

[說明]

桃園區網中心地址：(32001) 桃園市中壢區中大路300號-志希館 1 F
週一至週五：8-17時 電話：03-4227161 (分機轉 57555/57566)
週一至週五：17-22時 電話：03-4227161 (分機轉 57511)
電子信箱：tanet_ncu@ncu.edu.tw

公告時間	標題	公告內容	相關網址	附件
2019-10-18 13:46:51	[訊息轉發]【備用預警】Adobe Acrobat與Reader應用程式存在多個安全漏洞，允許攻擊者遠端執行任意程式碼，請儘速確認並進行更新	教育機構ANA通報平台 發佈編號 TACERT-ANA-2019101801 詳見全文		
2019-10-14 13:43:17	[會議]桃園區域網路中心管理委員會第64次會議暨資訊講座	桃園區域網路中心管理委員會第64次會議暨資訊講座 時間：108年11月1日 詳見全文	20191014_134317.zip 下載	
2019-10-08 17:20:29	[通知]NOC網路維護公告系統-[設備][計畫性維護]-TWAREN中央大學ASR模組擴充安裝，將影響服務約4小時	事由：因TWAREN中央大學GigaPOP ASR路由設備擴充安裝，需升級 詳見全文		
2019-10-07 09:41:14	[通知]【延期通知】NOC網路維護公告系統-[設備][計畫性維護]-TWAREN中央大學ASR模組擴充安裝，將影響服務約4小時	【延期通知】NOC網路維護公告系統-[設備][計畫性維護]-TWAR 詳見全文		

編號	項目	維護日期
156	TWAREN SDN 設備檢查/保養	2019/09/11
155	TWAREN 100G主機維護/保養	2019/08/08
154	TANet 100G-電池主機維護/保養	2019/08/08
153	TANet 100G-SMR主機維護/保養	2019/08/08
152	TANet 100G-RPM主機維護/保養	2019/08/08
151	TANet 100G主機維護/保養	2019/08/08
150	TWAREN 主機維護/保養	2019/08/06
149	TWAREN 主機維護/保養	2018/08/28
148	更換TWAREN網路量測主機	2019/06/28
147	TWAREN SDN 設備檢查/保養	2019/06/05
146	TWAREN 主機維護/保養	2019/05/07
145	TWAREN SDN 設備檢查/保養	2019/02/23
144	TWAREN 100G主機維護/保養	2019/02/21
143	TWAREN 主機維護/保養	2019/02/19
142	TWAREN 主機維護/保養	2018/11/29
141	TANet 100G-電池主機維護/保養	2018/11/13
140	TANet 100G-RPM主機維護/保養	2018/11/13
139	TWAREN 100G主機維護/保養	2018/11/13
138	TANet 100G主機維護/保養	2018/11/13
137	TANet 100G-SMR主機維護/保養	2018/11/13
136	TWAREN 100G主機維護/保養	2018/08/18
135	TANet 100G主機維護/保養	2018/08/15
134	TANet 100G-電池主機維護/保養	2018/08/15
133	TANet 100G-RPM主機維護/保養	2018/08/15
132	TANet 100G主機維護/保養	2018/08/15
131	TANet 100G-SMR主機維護/保養	2018/08/15
130	TWAREN 100G主機維護/保養	2018/05/23
129	TANet 100G-電池主機維護/保養	2018/05/23
128	TANet 100G-RPM主機維護/保養	2018/05/23
127	TANet 100G主機維護/保養	2018/05/23
126	TANet 100G-SMR主機維護/保養	2018/05/23
125	TWAREN 主機維護/保養	2018/05/09
124	TWAREN 主機維護/保養	2018/01/29
123	TWAREN 100G主機維護/保養	2018/01/29
122	TANet 100G-電池主機維護/保養	2018/01/29
120	TANet 100G-RPM主機維護/保養	2018/01/29
119	TANet 100G主機維護/保養	2018/01/29
118	TANet 100G-SMR主機維護/保養	2018/01/29
117	TWAREN 100G主機維護/保養	2017/11/29
116	TANet 100G-電池主機維護/保養	2017/11/29
115	TANet 100G-RPM主機維護/保養	2017/11/29
114	TANet 100G主機維護/保養	2017/11/29

桃園區網 管理委員會

- 管理委員會每半年召開一次，輪流到各連線單位開會，達到觀摩交流之目的
- 1月10日於國立中央大學召開第63次會議
 - 振聲中學 梁志清主任 經驗分享
 - 長庚大學 吳凱威老師 經驗分享
- 10月31日於長庚大學召開第64次會議
 - 大華中學 徐明添老師 經驗分享



桃園區網 傑出網路管 理人員選拔

- ❑ 108年桃園區網傑出網路管理人員，於10月31日桃園區網管理委員會第64次會議進行公開選拔程序。
- ❑ 經票選後，傑出網路管理人員當選人共計4名。
 - ❑ 永平工商高級中等學校王郁淵組長
 - ❑ 桃園市政府教育局張鈞富先生
 - ❑ 桃園市政府教育局陳瑞興管理師
 - ❑ 元智大學資服處網路媒體組劉興智組長



桃園區網 LINE群組

□ LINE群組可加強網路問題的即時發現與處理。

桃園區域網路中心連線單位

59 人

各位桃園區網夥伴好:

9月6日(五)

☆☆ ORANGE
請問..現在教育部dns有問題嗎? 下午 2:06

☆☆ ORANGE
國外mail收發有問題 下午 2:11

☆☆ ORANGE
分析edu.tw的 DNSSEC問題 下午 2:24

Domain	Check Results
tw	- 找到DnsKEY記錄 + - Ds = 20326 / SHA-256 驗證 DNSKEY = 20326 / SEP - 在DNSKEY RRset上找到1個RRSIG - RRSIG = 20326 * DNSKEY = 20326 / SEP 驗證 DNSKEY RRset
tw	- 在tw中找到1個DnsKEY記錄 + - Ds = 40792 / SHA-256 驗證 DNSKEY = 40792 / SEP - 在Ds RRset上找到1個RRSIG - RRSIG = 59944 * DNSKEY = 59944 驗證 Ds RRset - 找到DnsKEY記錄 + - Ds = 40792 / SHA-256 驗證 DNSKEY = 40792 / SEP - 在DNSKEY RRset上找到1個RRSIG - RRSIG = 40792 * DNSKEY = 40792 / SEP 驗證 DNSKEY RRset
edu.tw	- 在tw網域找到了2個關於edu.tw的DnsKEY記錄 - Ds = 40234 / SHA-256 驗證 DNSKEY = 40234 / SEP - Ds = 40234 / SHA-1 驗證 DNSKEY = 40234 / SEP - 在Ds RRset上找到1個RRSIG - RRSIG = 62955 * DNSKEY = 62955 驗證 Ds RRset - 找到4個DnsKEY記錄 + - 在DNSKEY RRset上找到1個RRSIG - RRSIG = 32734 * DNSKEY = 32734 / SEP 驗證 DNSKEY RRset - DNSKEY RRset未由信任鏈中的信任記錄簽名 - 在SOA RRset上找到1個RRSIG - RRSIG = 45533 * DNSKEY = 45533 驗證 SOA RRset

測試傳送到主頁 或 在網頁上查看測試結果

想要第二個意見嗎? 在測試edu.tw 測試結果

儲存 | 另存新檔 | 轉傳 | 貼文串 | Keep

Lu fangfa
@☆☆ ORANGE
已請教育部檢查 下午 2:35



協助連線學校 網路升級

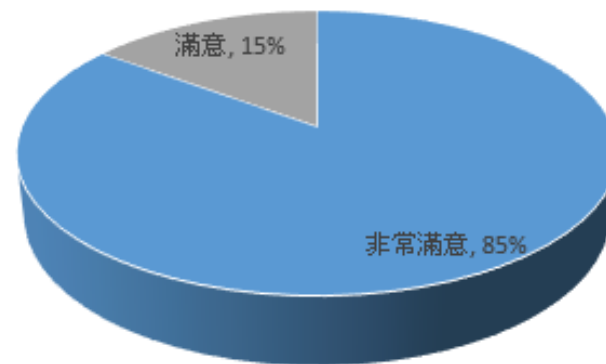
- 協助高中職連線學校由100M升速至300M，
月租不變。
- 已升級學校
 - ✓ 大華高中
 - ✓ 復旦高中
 - ✓ 六和高中

服務滿意度

● 填寫問卷學校：
34所

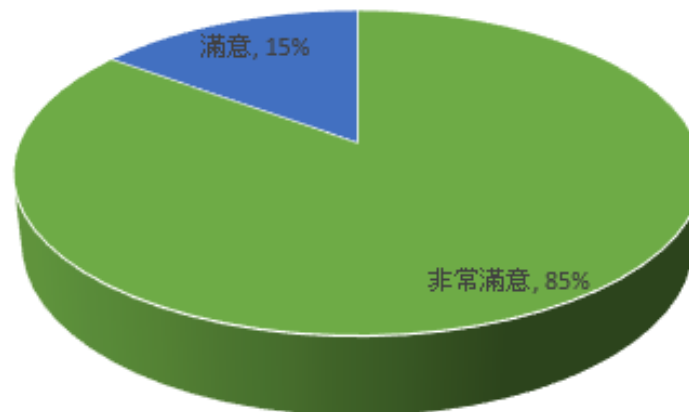
● 填答率：94%

對於區網中心處理問題的速度與回應
是否滿意？



■ 非常滿意 ■ 滿意

對於區網中心整體服務是否滿意？



■ 非常滿意 ■ 滿意

教育訓練推廣(1)

時間	主講人	課程名稱
108年01月10日	吳章銘先生 Fortinet台灣區技術總監	還要一直IoT嗎？IoT的整體安全防護
108年01月10日	楊光明先生 Fortinet 資深技術顧問	當SOC遇見NOC - 原來SIEM的使用也可以很簡單
108年04月15日	梁志清主任 振聲高中資訊室主任暨圖書館主任	Google+Arduino+Line+Appinventor 超乎你想像的免費工具
108年04月23日	張二川技正 國立中央大學	資訊安全面面觀
108年05月13日	魏宏吉 佐理研究員 國家高速網路與計算中心	桃園區域網路中心資安實作 Workshop 第一場 - 網站弱點評估實務



教育訓練推廣(2)

時間	主講人	課程名稱
108年06月03日	張育涵 先生 國家高速網路與計算中心	桃園區域網路中心資安實作 Workshop 第二場 -網路封包分析實務
108年08月16日	安興彥先生 國家高速網路與計算中心	桃園區域網路中心資安實作 Workshop 第三場 -源碼檢測實作
108年11月18日	吳惠麟先生 國立中山大學資訊管理系	桃園區域網路中心資安實作 Workshop 第四場 -開源碼主從式稽核記錄系統建置
108年12月23日	游子興先生 國立台灣大學計網中心	桃園區域網路中心資安實作 Workshop 第五場 -建置資安攻防演練平台- 從原理到實作

內壢高中 資安講習- 資訊安全 面面觀

- 108年04月23日(二)
- 前往連線學校內壢高中協助資安講習-資訊安全面面觀
- 講師：張二川技正/國立中央大學
- 課程大綱
 - (一)、資通安全法簡介
 - (二)、資訊安全威脅現況
 - (三)、電子郵件社交工程與案例
 - (四)、桃園區網介紹





五場資安實作 Workshop 系列課程

課程強調動手實作以加強學習成效。

第一場 網站弱點 評估實務

108.05.13 (一)
09:00~16:00

網站弱點評估實務

講師：魏宏吉 助理研究員/
國家高速網路與計算中心

上課人數：48人

課程大綱

課程著重在網站應用服務，
探討相關的安全性問題，
並且搭配Lab 讓學員學習
如何評估一個網站的安全性，
探討如何做好基本的
網站應用程式安全防範。



第二場 網路封包 分析實務

□ 108.06.03 (一)

09:00~16:00

□ 網路封包分析實務

□ 講師：張育涵先生/國家高速網路與計算中心

□ 上課人數：39人

□ 課程大綱

本課程將介紹網路通訊中常用通訊協定原理介紹、分析與應用，Wireshark 分析工具使用、熟悉 BFP 過濾器及常用操作技巧，進行網路攻擊封包分析。



第三場 源碼檢測 實作

□ 108.08.16 (五)

09:00~16:00

□ 源碼檢測實作

□ 講師：安興彥先生/國家高速網路與計算中心

□ 上課人數：45人

□ 課程大綱

為什麼常常聽到網站遭到駭客入侵，難道都是程式設計師故意製造的漏洞嗎？其實駭客不會乖乖使用你設計好的功能，要了解駭客的想法，才能寫出更安全的程式碼。





第四場 開源碼主 從式稽核 記錄系統 建置

- 108.11.18 (一) 09:00~16:00
- 開源碼主從式稽核記錄系統建置
- 講師：吳惠麟先生/國立中山大學資訊管理系
- 課程大綱
 - 本課程除了說明標準的稽核記錄格式外，另外也會探討如何利用開源碼社群的資源來即時將相關的稽核記錄匯入到資料庫。再使用SQL的語法來分析相關的稽核記錄。



第五場 建置資安 攻防演練 平台- 從 原理到實 作

- 108.12.23 (一) 09:00~16:00
- 建置資安攻防演練平台- 從原理到實作
- 講師：游子興先生/國立台灣大學計算機及資訊網路中心
- 課程大綱
 1. 資安攻防平台簡介
 2. 建置方式
 3. 漏洞的種類
 4. 入侵的方式
 5. 提升權限之方法
 6. 演練與實作。



推動網路 資訊應用 環境與導 入—IPv6 推廣

單位	routing支援IPv6	dns支援IPv6
桃園區網	routing OK	dns OK
國立中央大學	routing OK	dns OK
中原大學	routing OK	
銘傳大學	routing OK	dns OK
健行科技大學	routing OK	dns OK
萬能科技大學	routing OK	dns OK
開南大學	routing OK	
南亞技術學院	routing OK	dns OK
中央警察大學	routing OK	
國防大學	routing OK	dns OK
陸軍專科學校	routing OK	dns OK
私立復旦高級中學	routing OK	



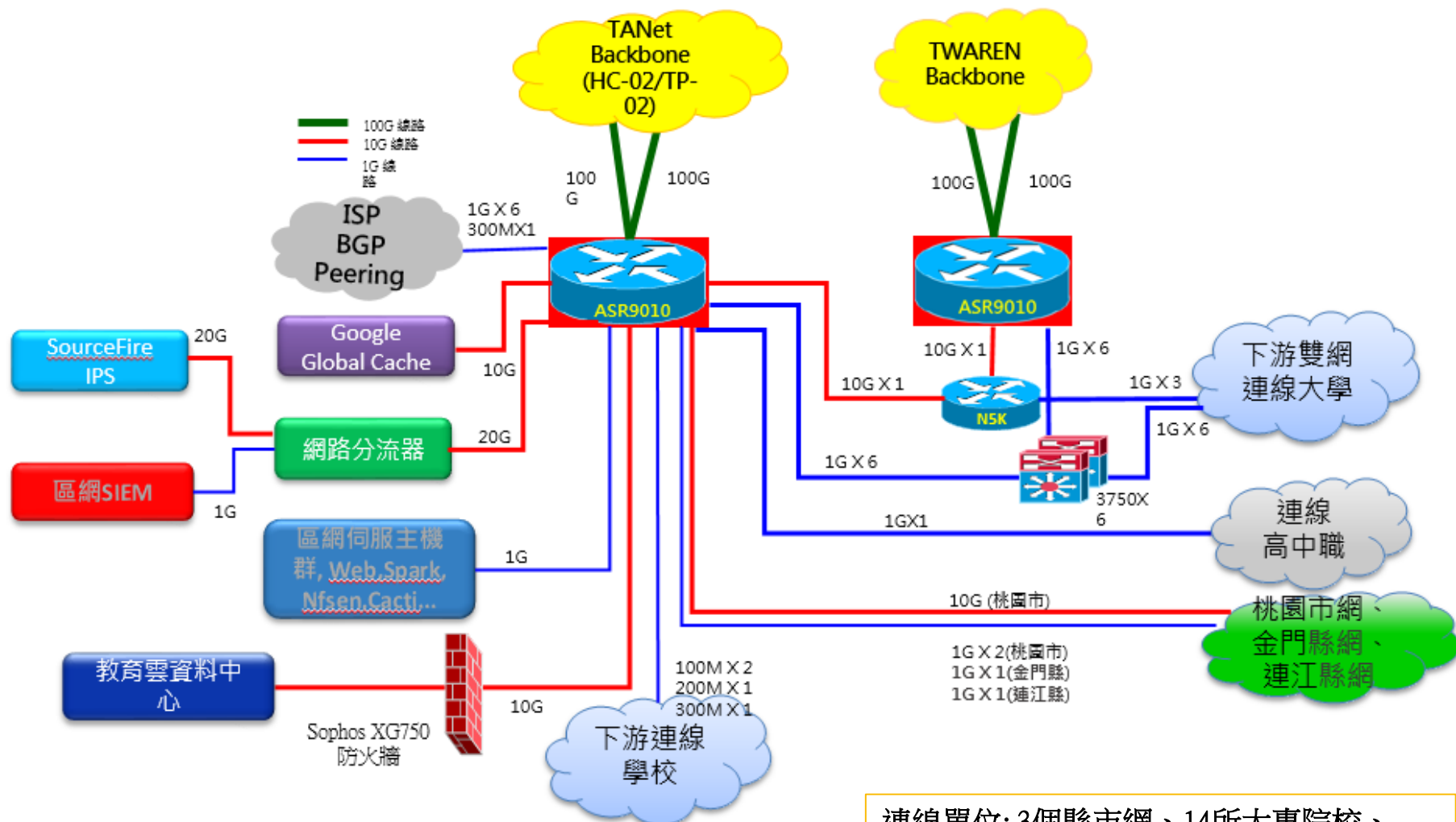
推動網路 資訊應用 環境與導 入—IPv6 推廣

單位	routing支援 IPv6	dns支援 IPv6
私立新興高級中學	routing OK	dns OK
桃園啟智學校	routing OK	
國立中壢高級商業職業學校	routing OK	dns OK
私立大興高級中學	routing OK	dns OK
核能研究所	routing OK	dns OK
國防大學理工學院	routing OK	dns OK
北區教育雲	routing OK	dns OK
桃園市網	routing OK	dns OK
桃園市楊明國小	routing OK	dns OK
連江縣網	routing OK	dns OK
金門縣網	routing OK	dns OK
金門大學	routing OK	dns OK
長庚大學	routing OK	
長庚科技大學	routing OK	
國立臺北商業大學-桃園校區	routing OK	dns OK

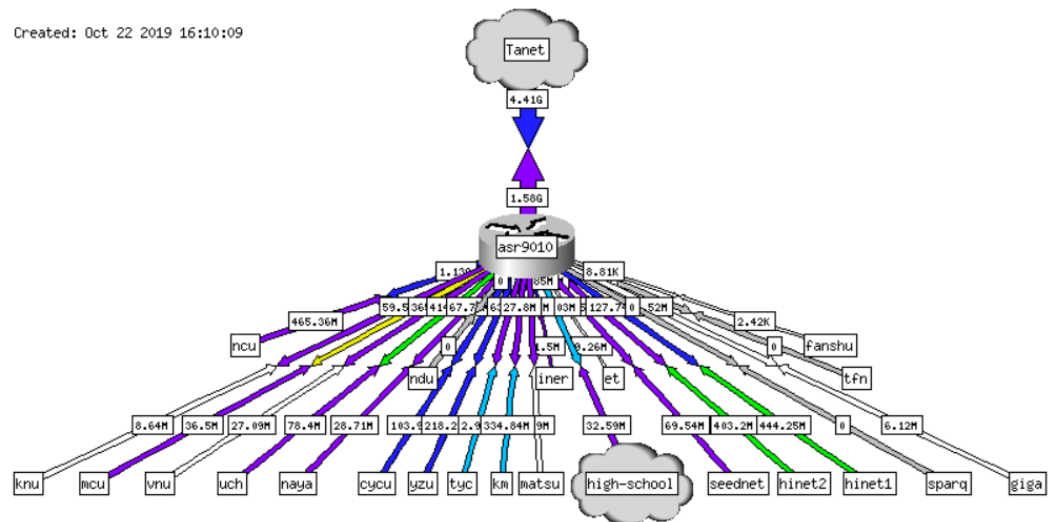
3.網路管理及資訊安全



桃園區網網路架構



連線單位: 3個縣市網、14所大專院校、
18所高中職、8個其他單位



<http://cacti.tyrc.edu.tw/tyrc.html>



桃園區網 高中職流 量

□ <http://cacti.tyrc.edu.tw/high-school.html>



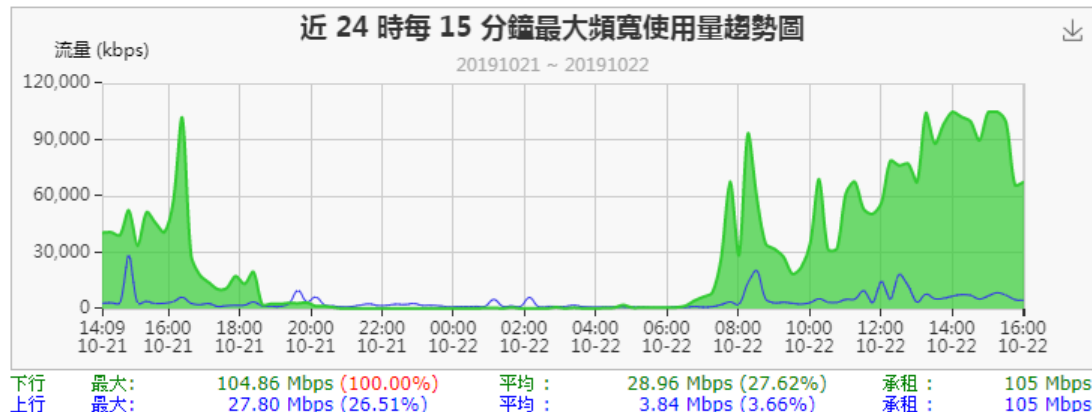
桃園區域網路中心

首頁

桃園區域連線 網路使用統計圖

1. 桃園農工 [FE]	2. 至善工商 [FE]	3. 新興高中 [FE]	4. 育達高中 [FE]
5. 治平中學 [FE]	6. 六和高中 [FE]	7. 中壢高中 [FE]	8. 啟英高中 [FE]
9. 永平工商 [FE]	10. 大興工商 [FE]	11. 復旦中學 [FE]	12. 成功工商 [FE]
13. 清華高中 [FE]	14. 振聲高中 [FE]	15. 大華中學 [FE]	16. 中央警察大學 [FE]
17. Uplink [GE]			

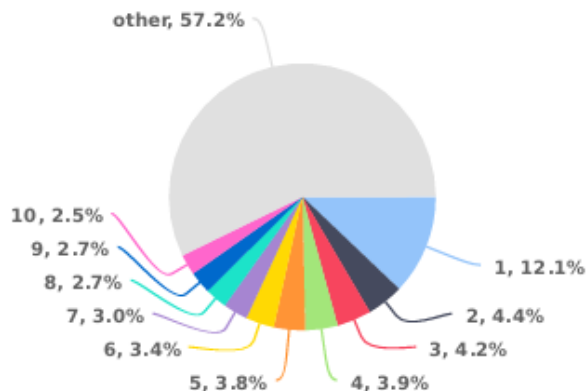
1. 私立六和高中 服務號碼：34YV000169 承租速度：100M/100M



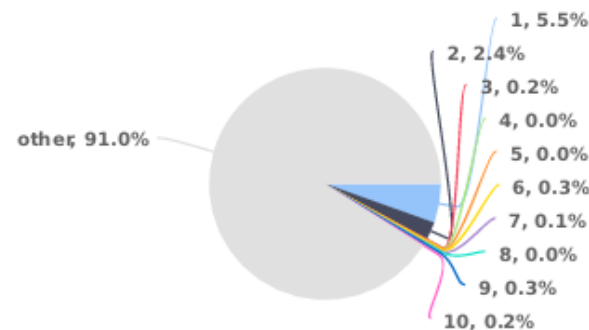


資安整備 —Top流量

Top 200 Byte
2019/10/29 00:00 ~ 2019/10/29 23:59



Top 200 Session
2019/10/29 00:00 ~ 2019/10/29 23:59

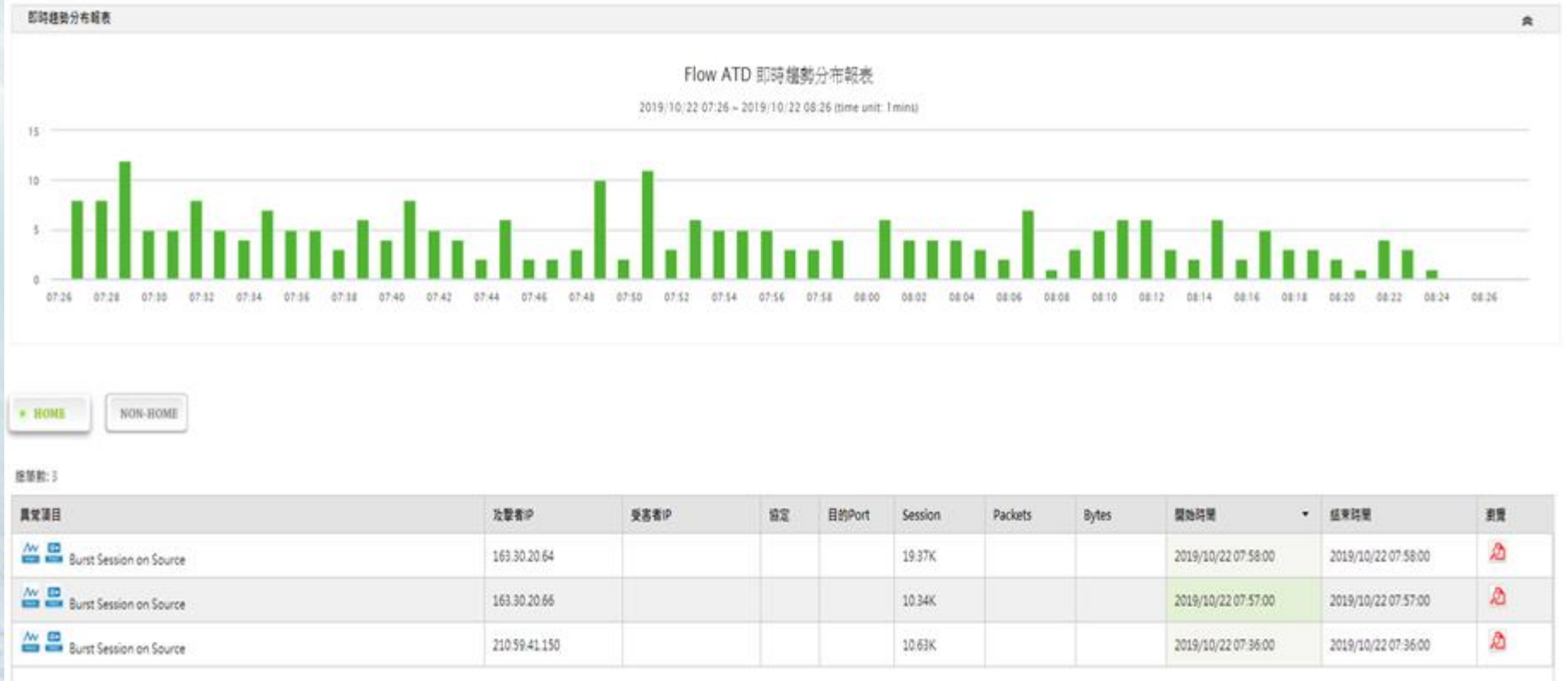


總筆數: 200

NO	來源 IP	來源名稱解析	HitCount	Session	Packets	Bytes
1	140.138.144.169	元智大學	0	2.16M	725.25M	8.79% 1,036G
2	140.115.50.87	中央大學	0	970.23K	696.11M	3.23% 380G
3	163.30.112.2	桃園市網	0	67.24K	286.78M	3.04% 358G
4	2001:288:3200:8:224:300:7481:aa74	桃園市網	0	2.35K	261.78M	2.87% 338G
5	2001:288:3200:8:224:200:d10:6075	桃園市網	0	3.23K	250.50M	2.74% 323G
6	163.30.4.38	桃園市網	0	115.31K	204.56M	2.5% 295G
7	163.30.40.120	桃園市網	0	51.73K	189.21M	2.18% 257G
8	2001:288:3200:8:195:300:6506:2c0	桃園市網	0	1.57K	178.61M	1.96% 230G
9	140.115.105.227	中央大學	0	127.23K	229.84M	1.95% 230G
10	120.124.96.250	逢行科技大學	0	86.39K	147.30M	1.81% 213G
11	140.115.0.198	中央大學	0	44.01K	133.60M	1.56% 184G
12	210.70.27.93	武陵高中	0	5.93K	136.44M	1.55% 183G
13	163.30.93.64	桃園市網	0	6.98K	126.40M	1.47% 174G
14	2001:288:3005:81:f0c2:c390:50a5:587	銘傳大學	0	4.76K	118.76M	1.35% 159G
15	210.71.45.3	國防大學	0	52.44K	135.58M	1.33% 156G



N-Reporter-異常流量告警





資安整備- ISMS資安 認證

- ❑ 桃園區網中心(中央大學)自2010年取得ISO27001認證後，每年均依規定接受複查以保持證照有效性；2019年3月通過ISO 27001:2017改版重新驗證。
- ❑ 提供臺灣學術網路桃園區域網路中心資訊安全技術相關之服務
- ❑ 轄下連線學校共有15個單位通過第三方認證
- ❑ 本中心共有19張ISO 27001:2013 LA、1張CISSP、4張CEH、3張CHFI等行政院國家資通安全會報公告之專業資安證照。

資安整備— 個資保護 驗證

- ❑ 中央大學於106年率先通過新版教育體系資通安全暨個人資料管理規範驗證，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23個一級單位擔任推動窗口，並已完成各一、二級行政學術單位導入BS 10012個人資料管理系統（PIMS），每年持續辦理個人資料管理制度教育訓練、內部稽核等相關活動。
- ❑ 同時也持續接受「教育機構資安驗證中心」的追查稽核以維持本校個人資料管理制度之有效性。



資安整備-桃園區網提供的檢測

- ❑ 資訊安全網站檢測系統
 - 提供桃園區網連線單位申請弱點掃描(IP)及網頁檢測(Web)檢測
 - 使用APP Scan及LANguard做為檢測工具
 - 檢測結果以E-mail加密方式通知申請者
- ❑ 定期追蹤申請單位是否針對弱點結果修正，修正後會再次執行掃描以確保弱點是否已修復。

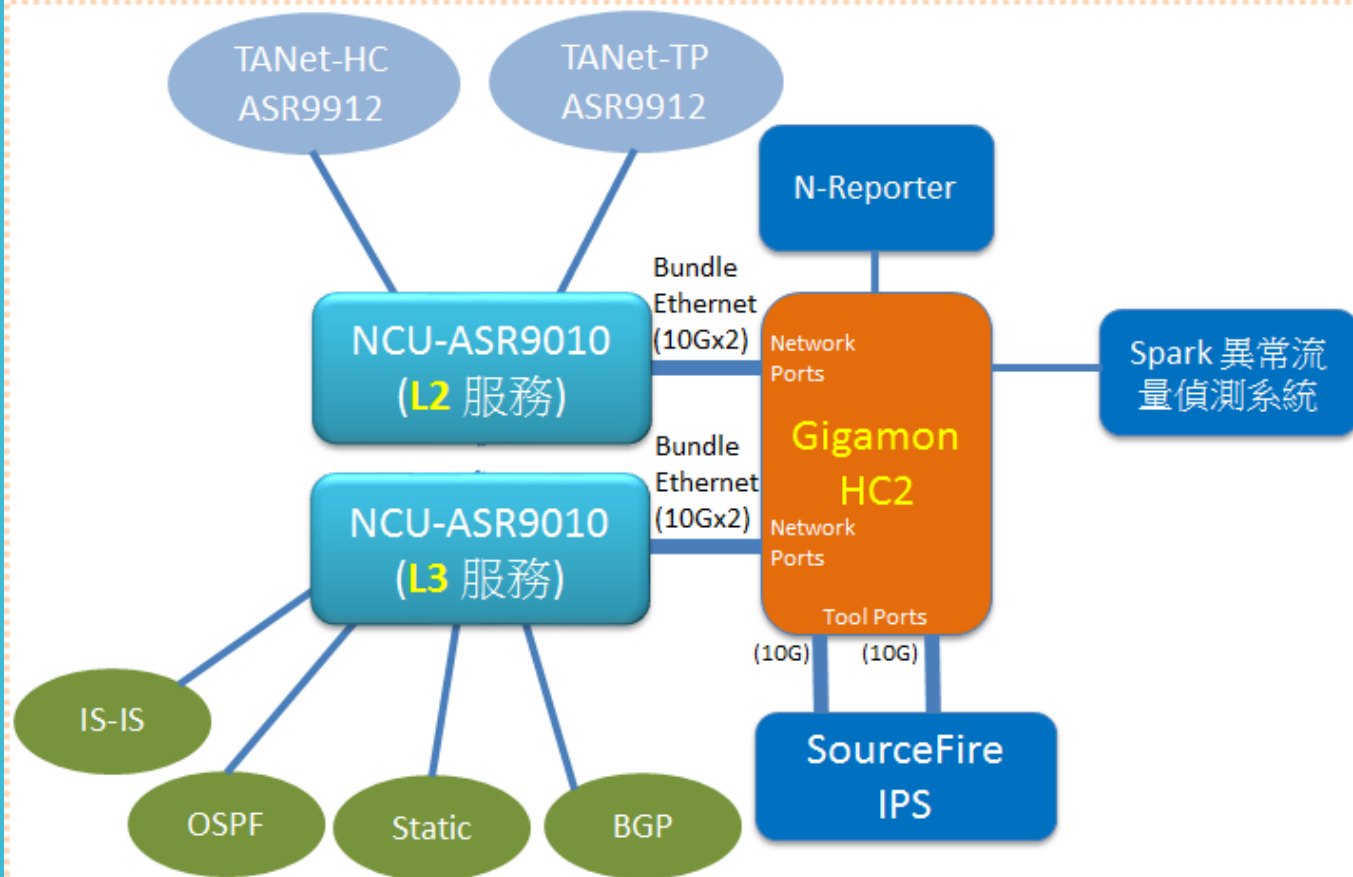
申請學校	弱點掃描(GFI LANguard)	網頁檢測(IBM APP scan)	追蹤處理情形
育達高中	5	3	已追蹤 2019/03/08
啟英高中	2	3	已追蹤 2019/03/12
萬能科技大學	3	4	已追蹤 2019/03/08
南亞技術學院	10	1	已追蹤 2019/03/08
中原大學	30	26	已追蹤 2019/03/11
龍潭高中	3	3	已追蹤 2019/09/18



資安整備- 桃園區網 提供的檢 測

申請學校	弱點掃描(GFI LANGuard)	網頁檢測(IBM APP scan)	追蹤處理情形
萬能科技大學	5	5	2019/09/18追蹤
中央警察大學	10	8	2019/09/20追蹤
新生醫護管理專科學校	8	0	2019/10/16追蹤
六和高中	5	3	2019/09/18追蹤
至善高中	5	3	2019/09/18追蹤
健行科技大學	5	1	2019/09/18追蹤
中壢高商	3	3	2019/09/18追蹤
新生醫護管理專科學校	2	2	2019/09/18追蹤
中原大學	37	13	2019/09/20追蹤
總計	133	78	已全數追蹤

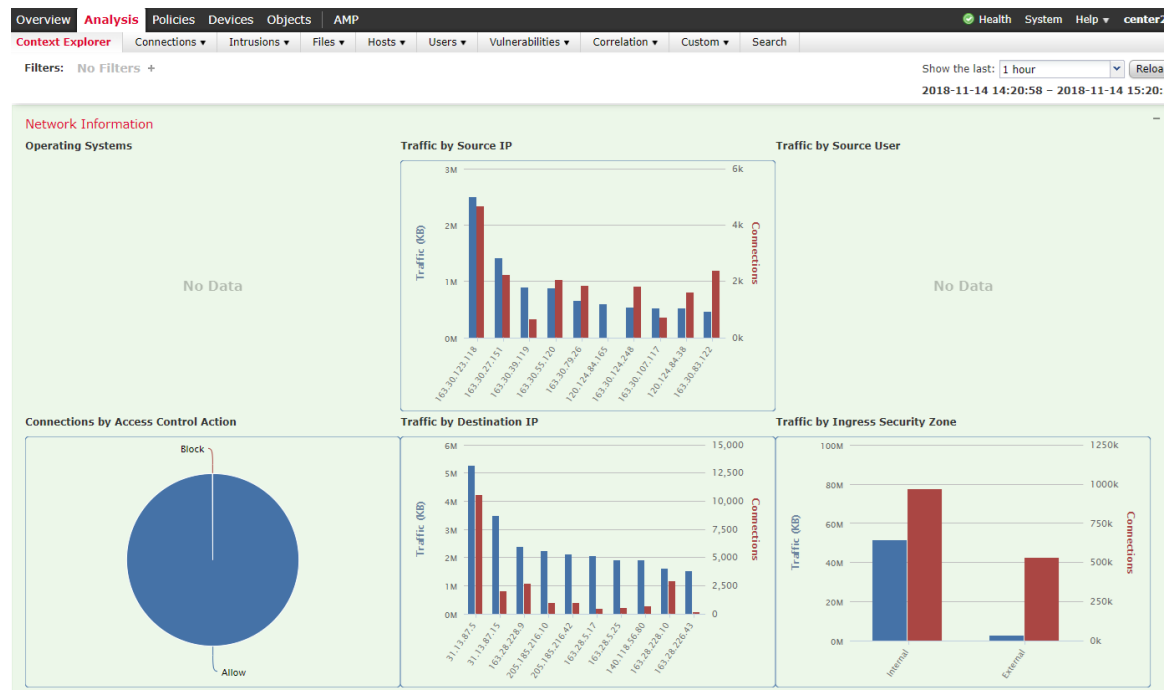
桃園區網 資安系統 架構



NCU-ASR9010與網路分流器架構

區網入侵防禦系統

- ☐ Cisco SourceFire IPS inline 運作，協助連線學校降低不當資訊的流竄、網路攻擊事件之發生，以提昇網路使用效率







重大營運 事件之檢討

事件	中央大學TWAREN骨幹設備中斷
事件說明	因季保養時，維護廠商誤觸供電設備導致TWAREN骨幹設備斷電重啟。
障礙時間	2019/02/21 10:30-10:39
事件檢討	1. 所有供電設備開關標示清楚。 2. 供電設備維護先提出維護步驟程序。 3. 廠商操作SMR時，必須回報國網中心執行動作。

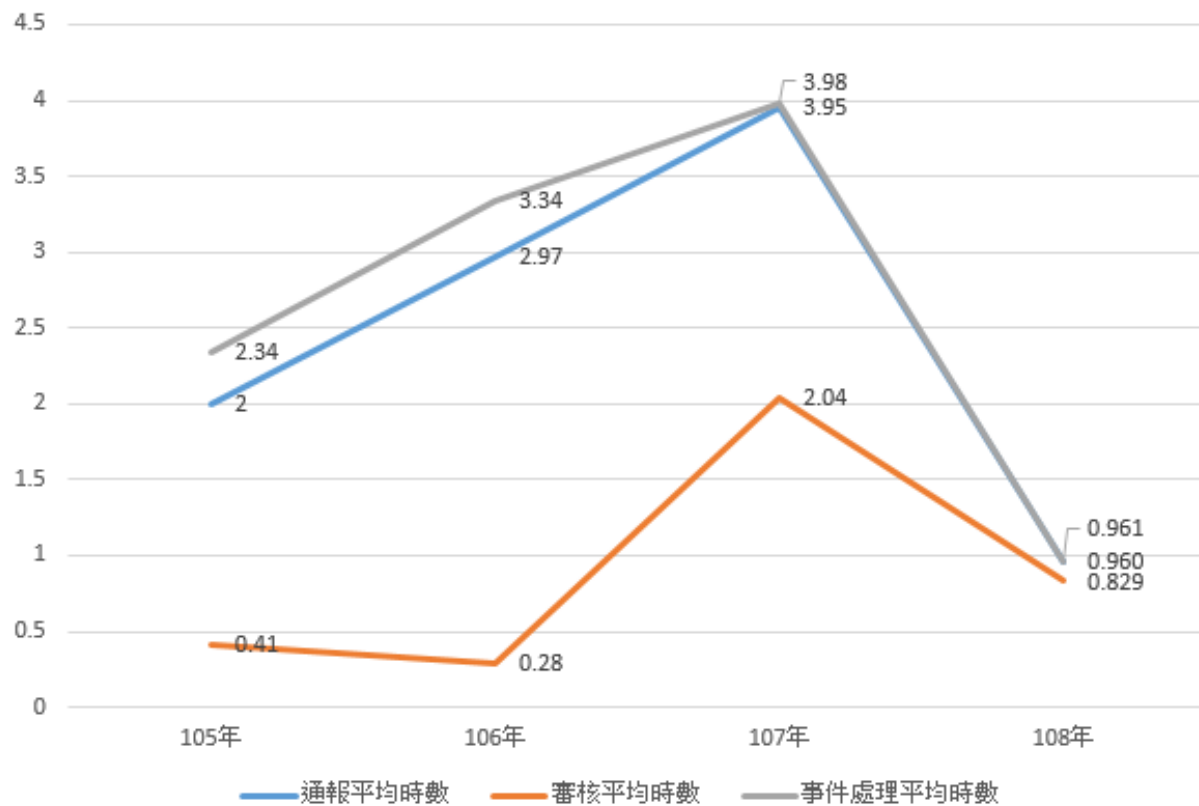


資安事件 統計

資料統計：2019/1/1-2019/10/25		桃園區域網路中心
1. 1、2級資安事件處理		
(1)通報平均時數：	小時	0.960
(2)應變處理平均時數：	小時	0.002
(3)事件處理平均時數：	小時	0.961
(4)通報完成率：	百分比	100%
(5)事件完成率：	百分比	99.668%
2. 3、4級資安事件通報		無
3. 資安事件通報審核平均時數：	小時	0.829
聯絡相關資訊完整度：	百分比	96.970%

歷年資安事件處理平均時數

桃園區域網路中心 1、2級資安事件處理平均時數

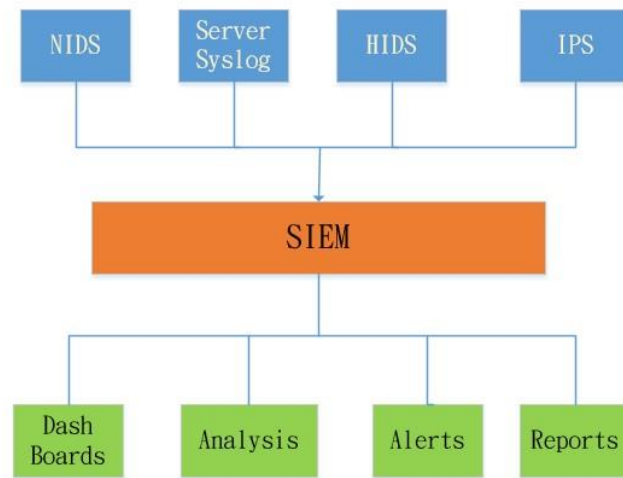


4.特色服務



開源軟體 系統之導入與應用 (1)

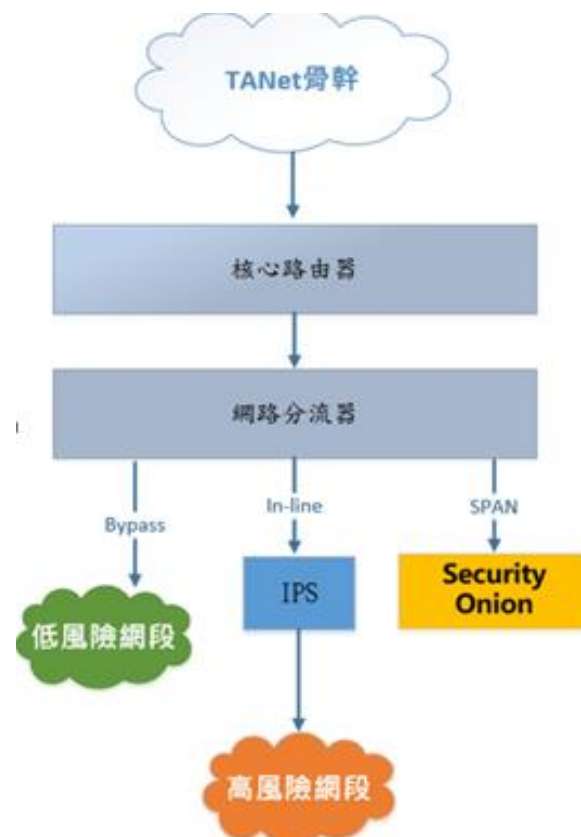
- 桃園區網中心透過導入開源OSSIM系統，即時監控網路行為並且針對HIDS、NIDS及IPS等系統事件收集、管理及分析，並分析事件之間的關聯。
- 藉由SIEM系統的視覺化儀表板、警示訊息、報表等功能，提供關連的資安事件，找出網路環境中的威脅。



TANET2018佳作論文獎

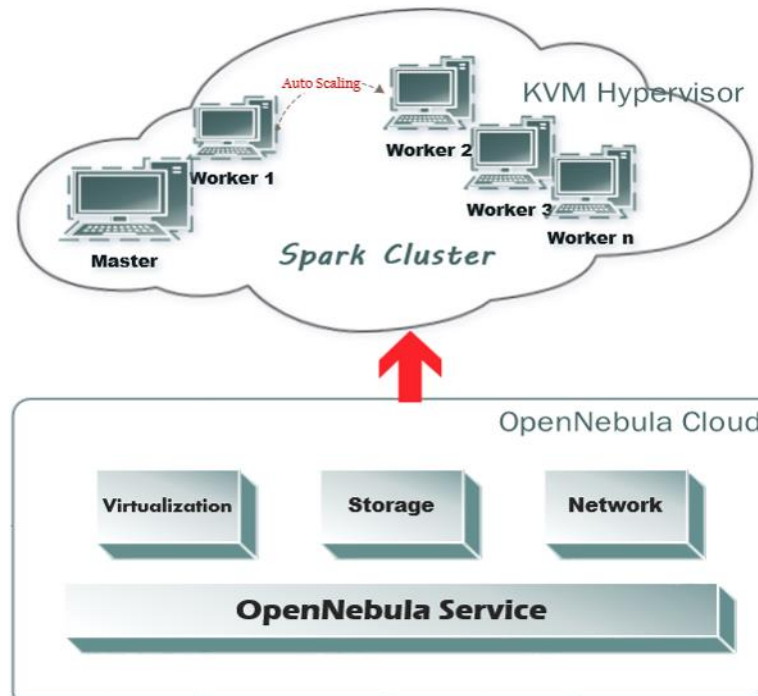
開源軟體 系統之導入與應用 (2)

- 導入 Security Onion系統，該系統成功地整合其他開源軟體，提供即時監控網路風險，並且提供網路入侵偵測系統及入侵防禦系統等功能。
- 藉由Sguil、Squert的GUI介面及警示訊息等功能，主動提供異常事件並以實際案例說明Security Onion找出挖礦主機的網路行為。



Spark異常 流量偵測 系統(1)

- 以自動化調整(auto-scaling)雲端架構搭配動態部署的Spark Cluster網路異常流量偵測系統，依照網路流量之大小自動調整Spark Cluster的計算節點數量。



推廣至花蓮區網及高屏澎區網



Spark異常 流量偵測 系統(2)

- 系統由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。



TANet桃園區網Spark+Hadoop流量監測 [\[連線學校 MRTG流量\]](#) [\[IPv6 MRTG流量\]](#) [\[Links 連線狀態偵測\]](#) [\[網管工具箱\]](#) [\[回](#)

TopN 流量排行 (小時)								
Keyword: Q Search								
Hostip	輸入量(MB)	輸出量	輸入連結	輸出連結	輸入封包長度	輸出封包長度	Duration(10分鐘)	紀錄時間
31.216.145.32@6	17	804	81	82	67	1498	2	11-07 10:00
31.216.145.46@6	33	424	23	21	169	1490	2	11-07 10:00
31.216.145.60@6	10	470	5	4	52	1499	1	11-07 10:00
34.102.131.225@6	9	536	8	9	44	1469	2	11-07 10:00
34.102.216.89@6	19	698	17	16	59	1469	2	11-07 10:00
34.80.57.157@6	54	5465	1000	707	44	1447	5	11-07 10:00
35.186.243.41@6	6	429	350	337	49	1440	5	11-07 10:00
35.186.245.167@6	8	406	208	209	54	1403	5	11-07 10:00
35.201.164.91@6	39	509	1979	2436	199	1249	5	11-07 10:00
35.221.162.160@6	63	1310	4321	4469	95	1300	5	11-07 10:00
35.227.255.143@17	6	778	166	201	73	1367	5	11-07 10:00
35.227.255.143@6	6	449	337	372	55	1429	5	11-07 10:00
35.244.140.142@6	8	1846	235	238	50	1457	5	11-07 10:00
36.226.93.62@6	18	934	94	97	43	1170	5	11-07 10:00
37.220.37.41@6	19	930	162	169	57	1473	5	11-07 10:00
38.106.72.51@6	7	509	173	183	47	1451	5	11-07 10:00
40.108.246.55@6	42	6626	65	66	41	1499	4	11-07 10:00

承辦108年 金門縣中 小學網管 人員校園 電腦維護 與管理研 習

▣ 108年10月5日(六) 9:00-16:40 由金門教育網路中心協辦，桃園區網中心率員前往金門縣教育網路中心電腦教室辦理研習。

▣ 議程表

09:00~09:10	開幕
09:10~11:10	校園網路管理
11:10~11:20	休息
11:20~12:20	網路連線分析
12:20~13:20	午餐
13:20~14:20	電腦網路安全
14:20~14:30	休息
14:30~16:30	資安檢測及 弱點掃描
16:30~16:40	Q&A





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

- VMware
- 虛擬化儲存軟體





教育雲上的服務系統詳細資源（按申請次序）

服務系統名稱	vm數量	vCPU	vRAM	vHD
數學小學堂系統	3	14	28	1304
中華開放教育平台	11	48	152	24528
體育雲-全民運動資訊系統	13	60	120	3948
體育雲-全民運動資訊系統報名網站	9	40	80	900
體育資訊雲端	3	12	24	300
教師研習平台	2	16	32	3272
臺灣微積分題庫	1	4	8	100
教育體系單一帳號驗證授權平臺	10	80	208	950
開放式教育資源系統	1	4	8	200
英語線上學習平台	2	16	32	3048
教育單位弱點檢測平台	1	8	16	100
寬橋測試機	2	2	4	200
教育媒體影音	6	24	48	9112
TANet VoIP	1	4	32	40
因材網	1	8	8	200
字形字音網	1	8	16	160
總計	67	348	816(GB)	47.2(TB)



教育雲北區雲端資料中心—資源使用情況

項目	*vCPU	vRAM (GB)	vHD(TB)
總資源量	216	1136	70
未使用資源	147.47	341.77	25.73
已使用量	68.53	794.23	44.27
已使用量(%)	31.73%	69.91%	63.24%

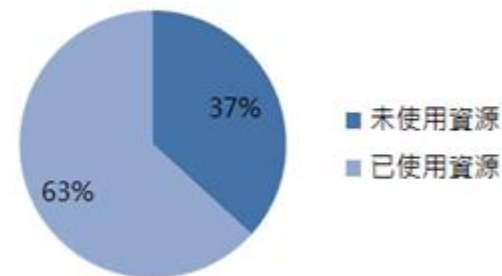
vCPU



vRAM



vHD





5 . 107年度缺失改善與精進



107年度執行成效評量改進意見項目成效精進情形(1)

107年度委員建議	改進及精進做法
建置問題集	建立網管、資安技術問題集FAQ，供連線學校查詢，可提供連線學校老師先自行排除問題，並節省區網人員回覆問題的工作量。
對本區網中心所連接的兩個離島縣網中心，建議可思考如何提供具創新服務特色的機制，如遠距視訊應用	繼續與金門、連江縣網中心合作開設網路管理一系列課程並視需要提供遠距視訊。
資安防護技術及人才之訓練建議針對高中職負責資訊人員每年進行教育訓練，或製作影音訓練課程，供高中職負責資訊人員自行學習。	本年度開設五場資安實作Workshop，並協助桃園市網中心辦理桃園市108年資訊組長研習計畫校園網路管理與網路流量分析課程。未來並配合現場環境及講師意願後將部分課程錄影以數位影音方式留存。
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。	本年度年終報告已加上網管及資安專案人員於區網業務之服務績效



107年度執行成效評量改進意見項目成效精進情形(2)

107年度委員建議	改進及精進做法
桃園區網中心亦同時擔任北區教育雲端資料中心, 建議對區網網路基礎運作機制環境評估其是否符合資料中心對外服務效能要求。	北區教育雲以10G頻寬連接桃園區網核心路由器, 其頻寬使用量在1G以下, 符合其對外服務效能及未來成長需求。
資安事件處理通報平均時數為3.924 小時, 事件處理平均時數為3.949 小時, 審核平均時數為2.035 小時, 較去年退步甚多, 建議了解問題處理改善之。	資安事件處理除透過自動轉通告系統即時通報連線學校, 二小時未填單以電話再度通知聯繫處理情形, 並針對超過24小時未處理的IP阻擋其連線。今年通報平均時數已降為 0.96 小時, 審核平均時數已降為為 0.829 小時。
服務單位中有金門及連江兩個離島縣網, 建議可多加了解其需求並予以協助。	今年已至金門協助研習課程, 並討論後續合作開設網路管理一系列課程。
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為97.06%, 建議加強至 100% 。	今年已加強通知, 但仍有連線學校老師公務繁重, 雖於2019年7月有變更密碼, 但並未被列入在統計區間內。

6 . 109年度預計推動之 重點工作



109年度預計推動之重點工作

- ❑ 協助提升連線學校資安防護技術及人才
- ❑ 持續與金門及連江縣網中心合作開設離島網管資安研習課程。
- ❑ 持續Spark異常流量偵測系統更新及對區網主幹轉送封包之監聽/分析/攻擊偵測。
- ❑ 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。
- ❑ 開源軟體系統之導入與應用。
- ❑ 增設高中職不當資訊過濾設備，預防學生使用學校網路會接觸到不當資訊。
- ❑ 自109年度開始，連線單位如有臨時需資安檢測可隨時向桃園區域網路中心申請。



7. 綜合建議





綜合建議

- ❑ 希望能支援高中職資安設備經費。
- ❑ 資訊安全相關服務，本來要花錢請外面公司做的，希望能有免費的服務可以協助。

臺灣學術網路-桃園區網中心



Thank You!