桃園區域網路中心110年度執行成效報告

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: 2021/11/19

2021

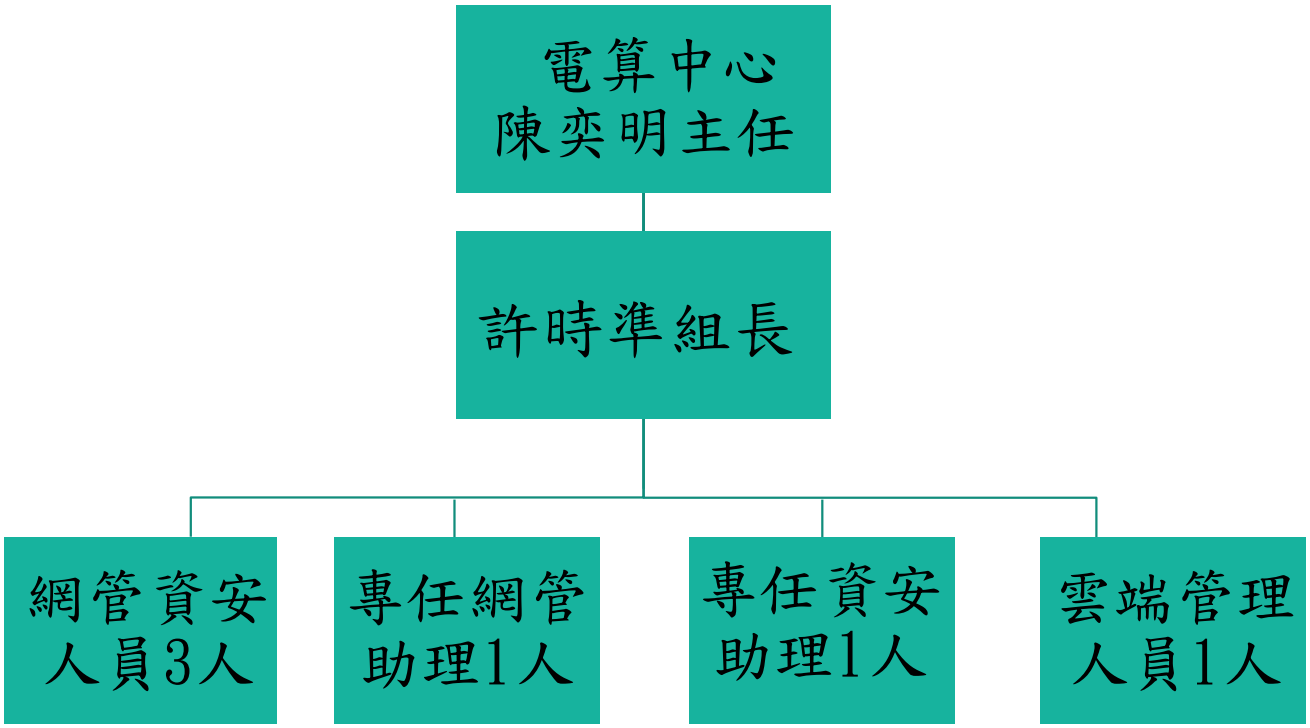
簡報大綱

1. 經費與人力
2. 網路管理
3. 資安服務
4. 特色服務、未來營運方針
5. 成效精進、KPI

第一章

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	4,915,500
教育部補助金額	3,655,500
自籌金額	1,260,000
實際累計執行數（至11月）	89.09%

107-109經費使用達成率

年度	計畫經費(核定數)執行率	計畫補助金額執行率
107年	95.44%	93.76%
108年	98.91%	98.52%
109年	99.99%	99.99%

(一)本中心積極推動計畫規劃項目，同時本撙節原則及落實經費管控，確實執行計畫補助經費，107~109年計畫核定經費執行率均達95%以上。

(二)依107年、108年度繳回人事費差額，均因人事費經費編列時概估隔年度雇主負擔勞、健保調整額度，及進用專任助理學經歷(職級)之差異所造成之賸餘數。

(三)自109年度起，計畫進用3名專任助理均依原編列職級聘用，故已無人事費賸餘數。

專任網管人員任務與績效

網管人員(1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。

專任資安人員任務與績效

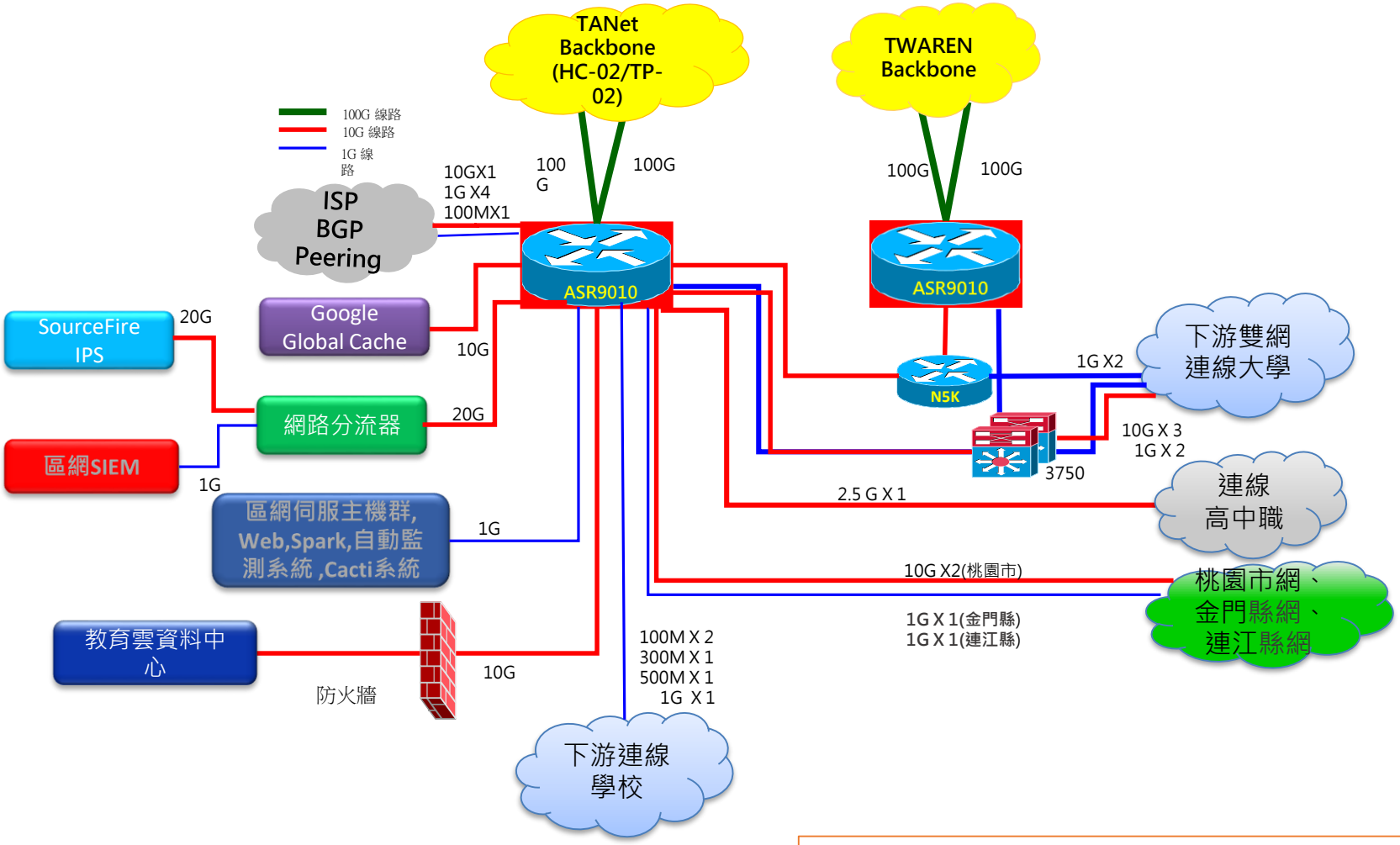
資安人員(1位)的任務與績效
資安通報審核及演練，資安事件處理
異常流量IP偵測及處理
協助ISO27001資安認證,個資保護系統維護
弱點掃描，網頁檢測及追蹤處理
辦理資安研討會，臨時交辦事項。

第二章

國立中央大學

網路管理

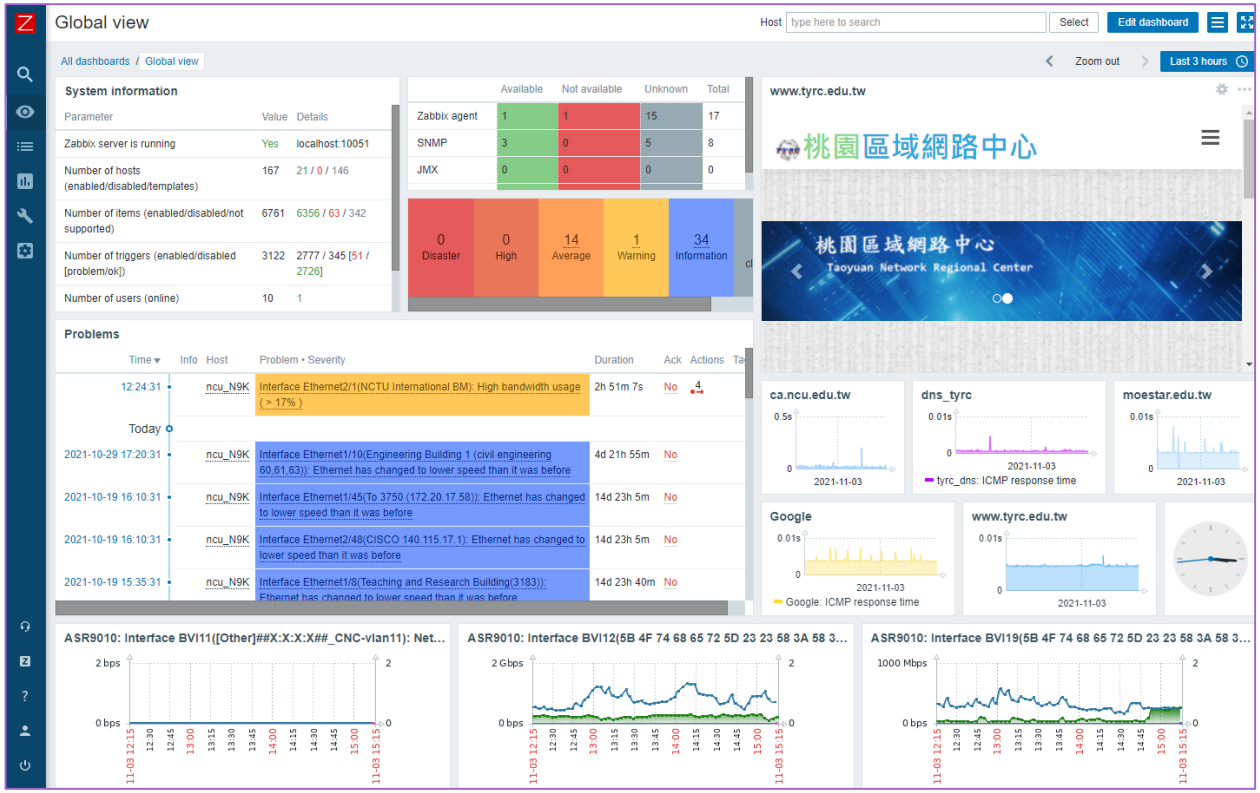
桃園區網網路架構



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

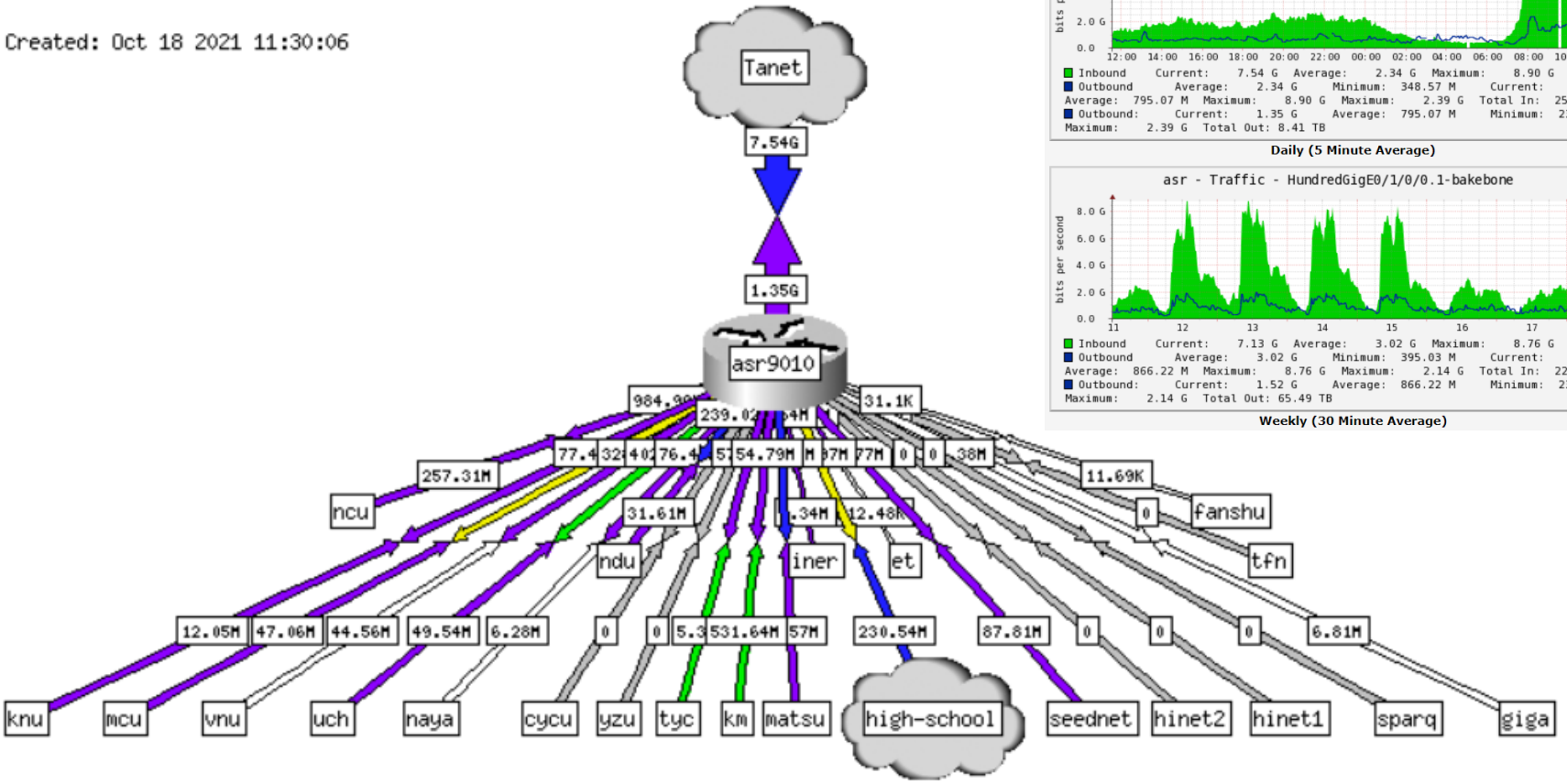
自動監測系統結合自行開發LINE Notify

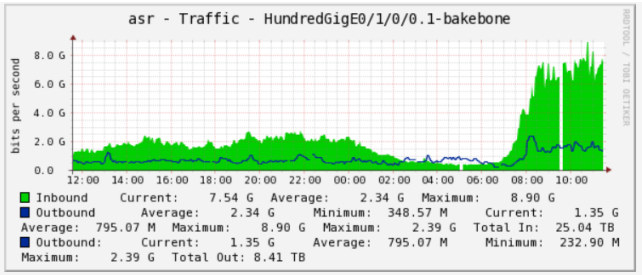
- 建置開源自動監測系統，針對重要網路設備、機房溫溼度監測、實體及虛擬伺服器的服務效能，利用自動化程序監測。並自行開發LINE Notify程式，進行LINE即時訊息自動發送警示訊息，讓網管人員及早發現問題並立即處理。

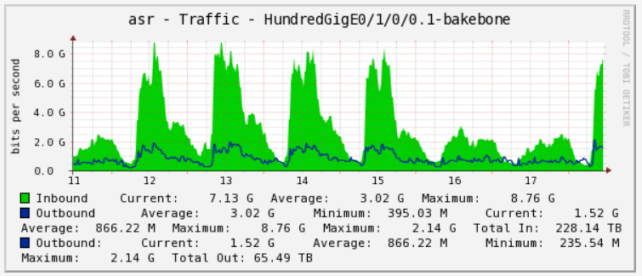


https://zabbix.tyc.edu.tw/

桃園區網Cacti系統監控流量

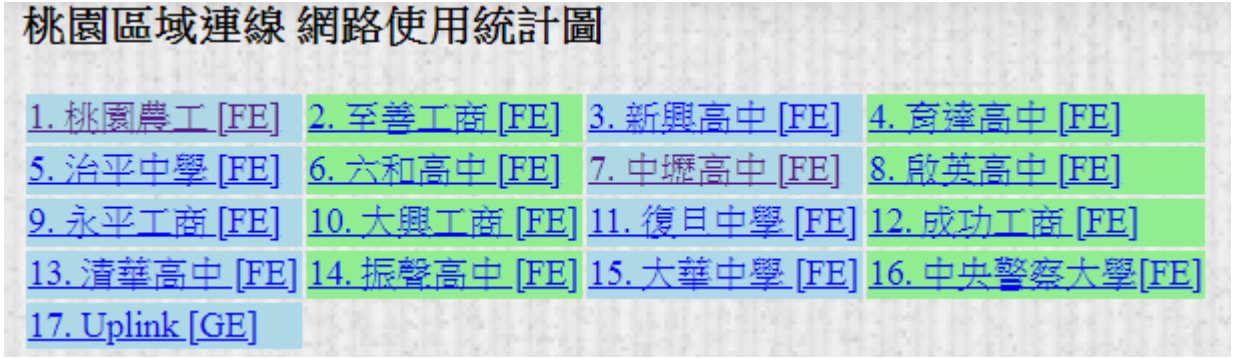


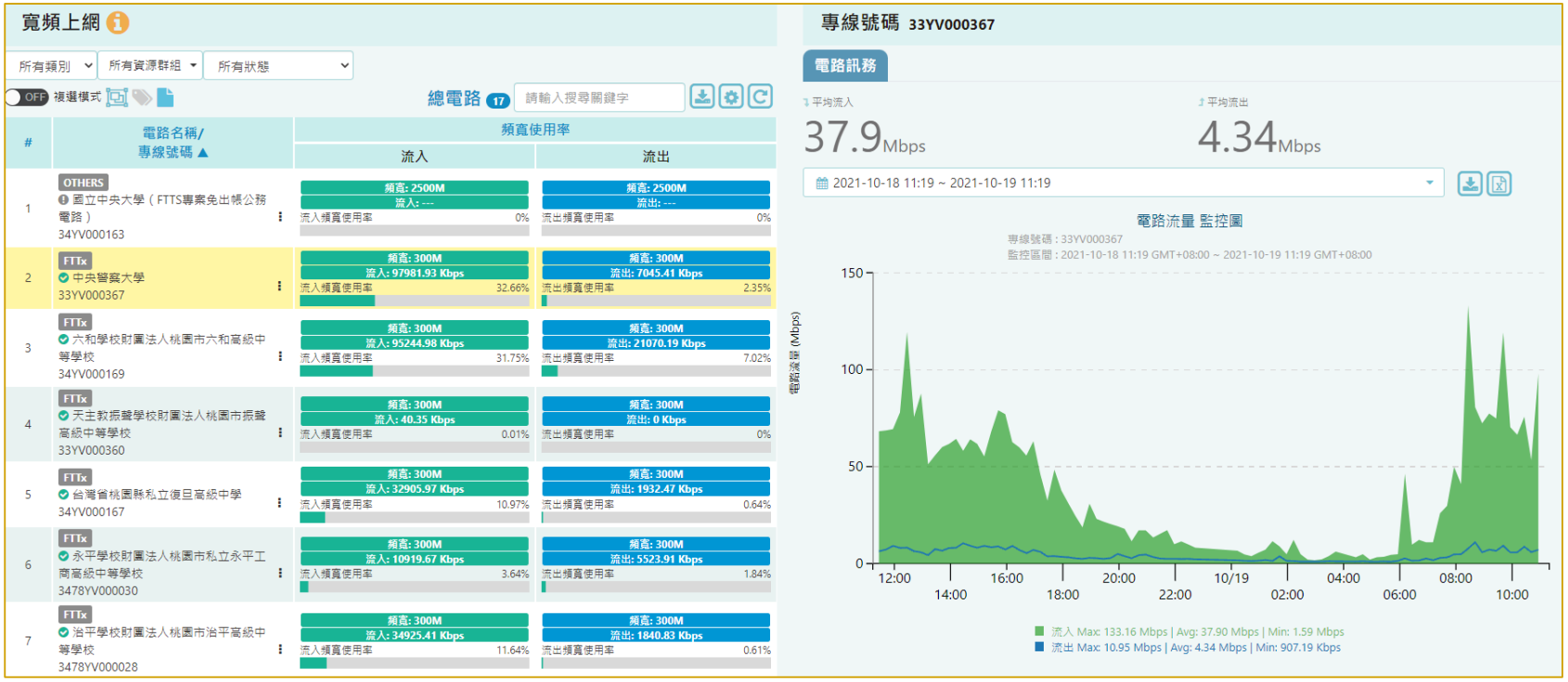




https://cacti.tyrc.edu.tw/tyrc.html

桃園區網高中職流量

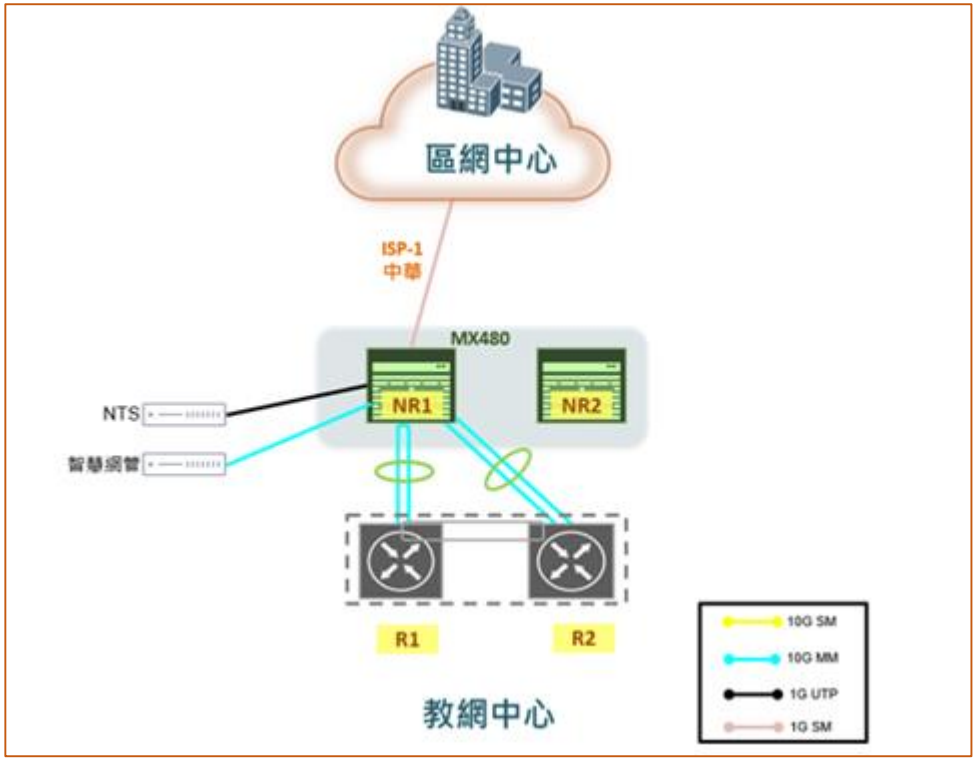




https://cacti.tyrc.edu.tw/high-school.html

協助教網中心進行骨幹設備更新

- 2021/08/11 18:00 協助金門縣網中心骨幹設備更新
- 2021/08/18 18:00 協助連江縣網中心骨幹設備更新
- 2021/08/30 18:00 協助桃園市網中心骨幹設備更新



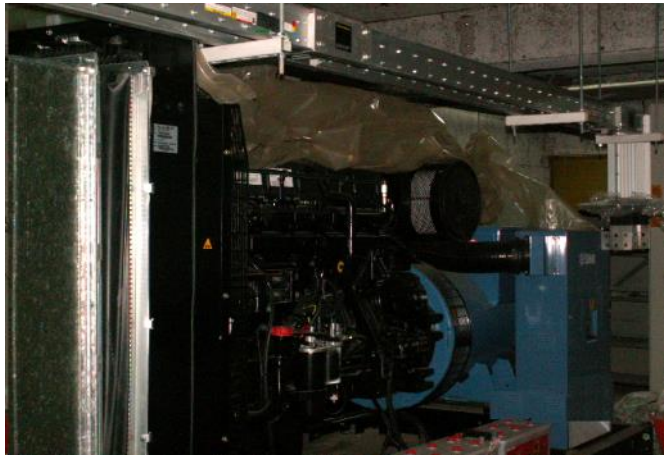
建置桃園區網中心網站常見問題FAQ

- 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。

https://www.tyrc.edu.tw/

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
  - 具450KVA發電機組及500KVA發電機組共2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



桃園區網維運—機房管理

- 訊息公告，重要訊息並以Email寄送、LINE公告至各連線單位
- 機房工作日誌

維護編號	維護事項	維護日期
TWAREN20210928-1	TWAREN SDN 設備檢查/保養	2021-09-28
TWAREN20210826-1	TWAREN 主機維護/保養	2021-08-26
TANET20210804-4	TANet 100G-電池主機維護/保養	2021-08-04
TANET20210804-3	TANet 100G-SMR主機維護/保養	2021-08-04
TANET20210804-2	TANet 100G-RPM主機維護/保養	2021-08-04
TANET20210804-1	TANet 100G主機維護/保養	2021-08-04
TWAREN20210804-1	TWAREN 100G 主機維護/保養	2021-08-04
TWAREN20210607-1	TWAREN SDN 設備檢查/保養	2021-06-07
TWAREN20210511-1	TWAREN 主機維護/保養	2021-05-11
TWAREN20210505-1	TWAREN 100G 主機維護/保養	2021-05-05
TANET20210505-4	TANet 100G-電池主機維護/保養	2021-05-05
TANET20210505-3	TANet 100G-SMR主機維護/保養	2021-05-05

https://www.tyrc.edu.tw/

桃園區網管理委員會

- 管理委員會每半年召開一次，並輪流到各連線學校開會，達到觀摩交流之目的。
- 4月29日於萬能科技大學召開第67次會議
  - 資安宣導及業務報告
  - 第二屆傑出網管人員頒獎
  - 桃園市網、臺北商業大學老師經驗分享
- 10月28日於健行科技大學召開第68次會議
  - 資安宣導及業務報告
  - 第三屆傑出網管人員選拔
  - 六和高中、陸軍專科學校老師經驗分享

桃園區網第三屆傑出網路管理人員選拔

- 2021/10/29 桃園區網第三屆傑出網路管理人員選拔，當選人如下
  - 元智大學　　鍾秉儒技佐
  - 桃園市北湖國小　黃哲緯先生
  - 方曙商工　　林瑞棋組長
  - 國立中央大學　周小慧資料管理師

桃園區網LINE群組

- 網路連線問題的即時發現與處理
- 病毒或網路攻擊訊息的即時分享
- 加強連線學校間的經驗分享與互相切磋

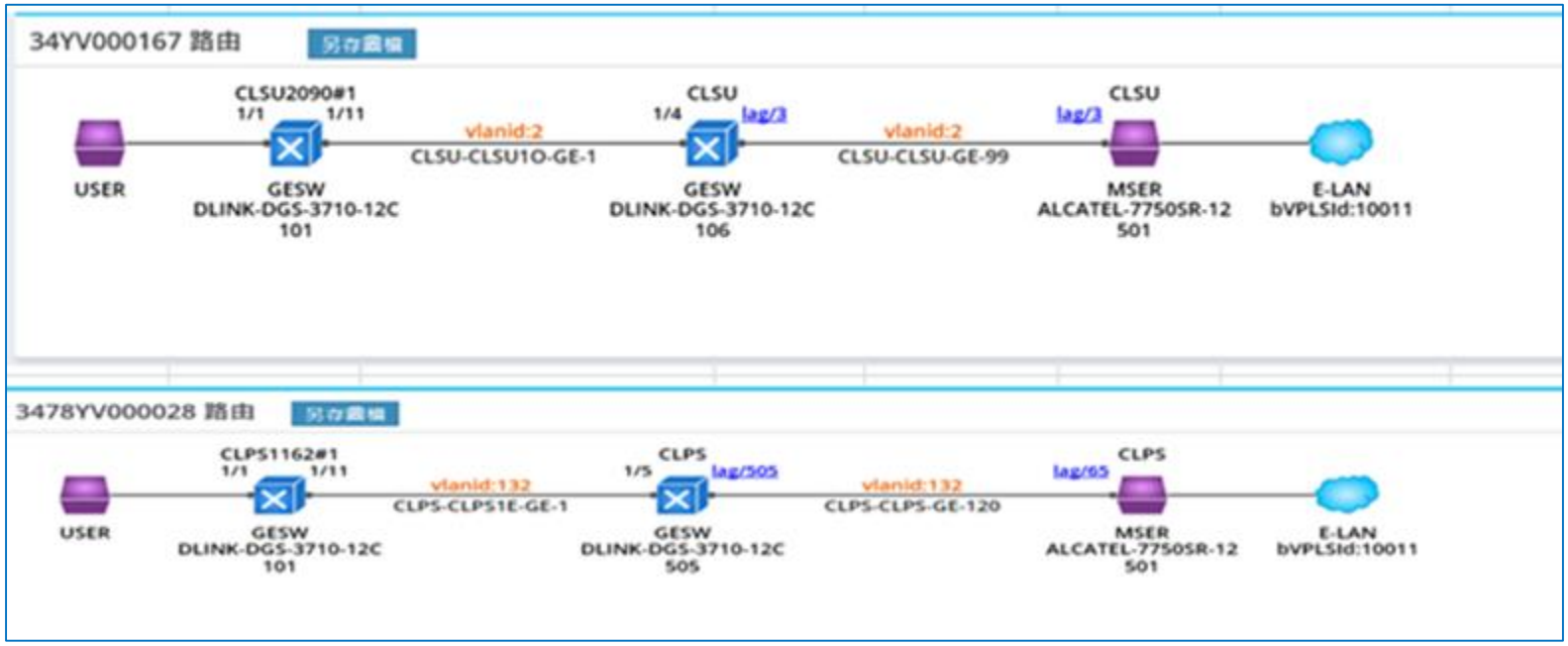
積極協助連線學校導入IPv6網路環境

- 2020年完成4所學校導入IPv6，2021年協助下列4所學校完成IPv6導入，另有2所完成設定，但仍有連線問題。
  - ✓ 中原大學於2021年4月26日完成導入IPv6。
  - ✓ 啟英高中於2021年5月14日完成導入IPv6。
  - ✓ 六和高中於2021年7月16日完成導入IPv6。
  - ✓ 國立體育大學於2021年10月19日完成導入IPv6。

積極協助連線學校導入IPv6網路環境

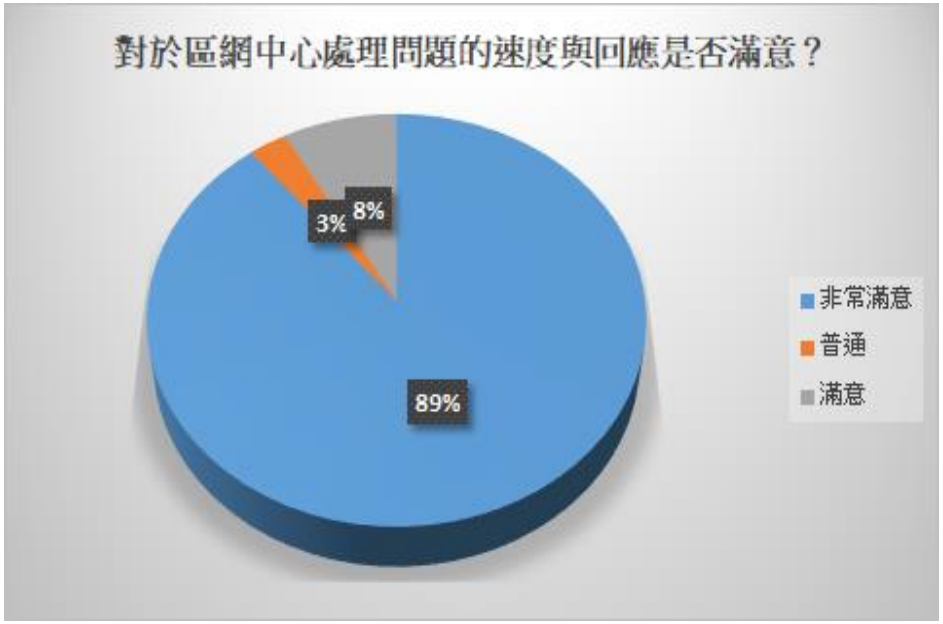
- 大華高中、治平高中學校端與區網端已完成IPv6設定，目前正請中華電信查修該公司機房Layer2設備IPv6不通問題(附圖為中華電信機房查修線路圖)。

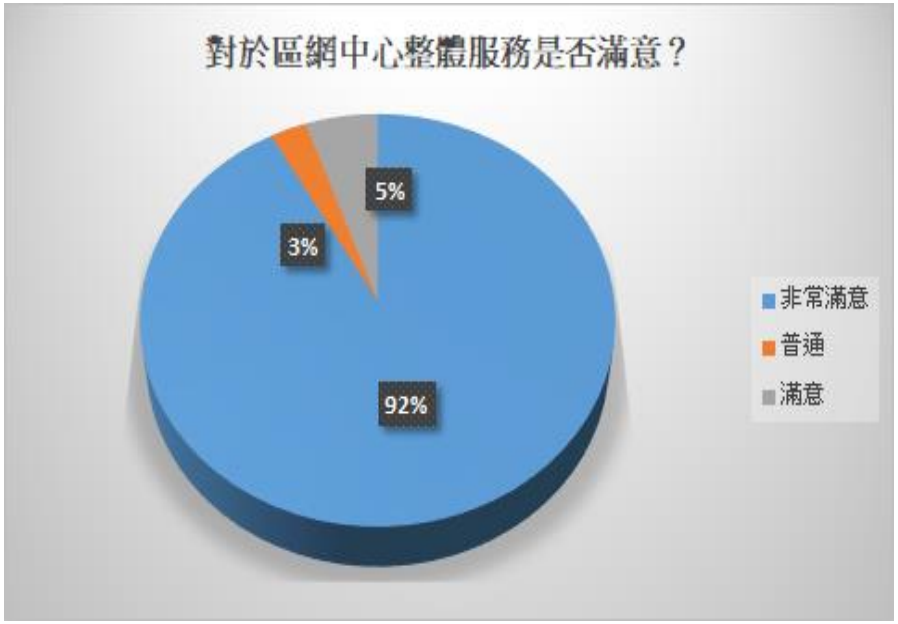
學校名稱	專線	IPV6
復旦中學	34YV000167	2001:288:30FF:100::11/64
治平高中	3478YV000028	2001:288:30FF:100::15/64



服務滿意度調查

- 填寫問卷學校：34所





桃園區網雲端資源提供連線學校VM

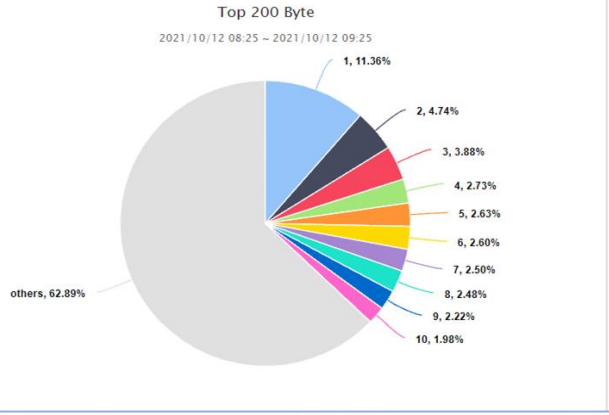
學校名稱	虛擬機數量
新生醫專	1台
核能研究所	2台
內壢高中	1台
中壢家商	1台
永平工商	1台
陽明高中	1台
金門大學	1台

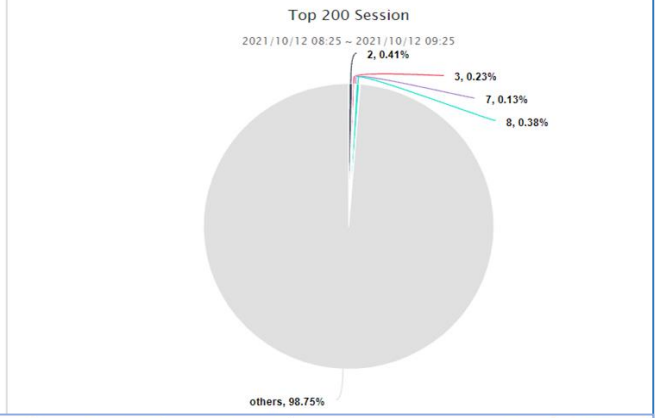
第三章

國立中央大學

資安服務

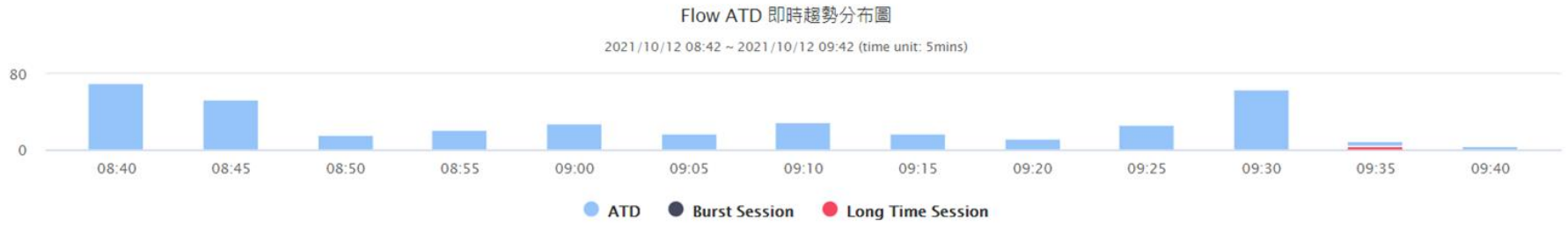
資安服務—Top流量





NO	來源 IP	來源 IP 名稱解析	Hit Count	Sessions	Packets	Bytes	流量圖
1	2001:288:3200:8:342:200:5586:a307	桃園市網	0	2.73K	50.19M	59.05G 11.36%	
2	163.30.125.25	桃園市網	0	44.54K	19.88M	24.64G 4.74%	
3	163.28.52.125	edu-cloud	0	25.29K	13.74M	20.13G 3.88%	
4	2001:288:3200:8:340:200:2ad0:f928	桃園市網	0	1.55K	10.61M	14.17G 2.73%	
5	2001:288:3200:10:343:224:93ff:f4a8	桃園市網	0	421	10.06M	13.65G 2.63%	
6	2001:288:3200:8:204:200:cc47:671f	桃園市網	0	565	10.72M	13.50G 2.6%	
7	163.30.40.23	桃園市網	0	14.61K	8.98M	12.98G 2.5%	
8	140.115.54.243	中央大學	0	41.08K	8.92M	12.88G 2.48%	
9	140.115.39.131	中央大學	0	4.17K	8.05M	11.53G 2.22%	
10	2001:288:3200:8:165:200:3a0a:ec01	桃園市網	0	1.11K	7.28M	10.27G 1.98%	
11	120.124.84.36	萬能科技大學	0	72.37K	13.31M	10.15G 1.95%	
12	2001:288:3200:8:309:200:9b17:af3a	桃園市網	0	389	5.81M	8.46G 1.63%	
13	163.30.182.65	桃園市網	0	14.44K	6.09M	7.66G 1.47%	
14	140.135.108.57	中原大學	0	559	5.95M	7.27G 1.4%	
15	2001:288:3001:60:3444:6cb5:c509:b	中央大學	0	1.19K	5.13M	6.40G 1.23%	
16	163.30.190.3	桃園市網	0	17.21K	4.21M	5.29G 1.02%	
17	210.60.236.4	龍潭高中	0	67.74K	6.48M	4.81G 0.92%	

資安服務—異常流量告警



IP 範圍： 全部

異常項目	攻擊者 IP	攻擊者區域	受害者 IP	受害者區域	協定	目的 Port	Session	Packet	Byte	開始時間	結束時間	瀏覽
TCP SYN Host Scan	134.122.90.83	DE			TCP	30127	143.25K	143.25K	7.55M	2021/10/12 09:33	2021/10/12 09:41	
TCP SYN Host Scan	106.12.36.109 (Baidu (China))	CN			TCP	6379	22.28K	22.28K	1.61M	2021/10/12 09:41	2021/10/12 09:41	
TCP SYN Host Scan	167.172.161.44	DE			TCP	30113	75.9K	75.9K	4M	2021/10/12 09:34	2021/10/12 09:41	
TCP SYN Host Scan	161.35.195.239	DE			TCP	30129	196.16K	196.16K	10.34M	2021/10/12 09:33	2021/10/12 09:41	
TCP SYN Host Scan	164.90.194.222	NL			TCP	30106	157.67K	157.67K	8.31M	2021/10/12 09:33	2021/10/12 09:41	
TCP SYN Host Scan	161.35.195.236	DE			TCP	30139	142.34K	142.34K	7.51M	2021/10/12 09:33	2021/10/12 09:41	
TCP SYN Host Scan	161.35.19.209	DE			TCP	30138	204.23K	204.23K	10.77M	2021/10/12 09:32	2021/10/12 09:41	
TCP SYN Host Scan	104.248.168.116	GB			TCP	30120	160.58K	160.58K	8.47M	2021/10/12 09:33	2021/10/12 09:41	
TCP SYN Host Scan	161.35.203.53	DE			TCP	30131	173.16K	173.16K	9.13M	2021/10/12 09:33	2021/10/12 09:41	
TCP SYN Host Scan	134.209.221.120	US			TCP	6026	49.43K	49.85K	2.63M	2021/10/12 09:41	2021/10/12 09:41	
TCP SYN Host Scan	161.35.19.131	DE			TCP	30134	79.55K	79.55K	4.2M	2021/10/12 09:33	2021/10/12 09:41	
TCP SYN Host Scan	128.199.232.131	SG			TCP	9110	225.78K	225.78K	11.91M	2021/10/12 08:43	2021/10/12 09:41	
TCP SYN Host Scan	142.93.46.186	GB			TCP	30121	141.62K	141.62K	7.47M	2021/10/12 09:33	2021/10/12 09:41	
TCP SYN Host Scan	157.245.192.18	SG			TCP	13787	249.39K	249.39K	13.15M	2021/10/12 08:48	2021/10/12 09:41	
TCP SYN Host Scan	161.35.198.221	DE			TCP	30112	98.02K	98.02K	5.17M	2021/10/12 09:33	2021/10/12 09:41	

25 第 1 共15頁 顯示1到25,共369記錄

資安服務-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；2021年3月通過ISO 27001:2017 定期驗證。
- 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18個學校通過資安第三方認證。
- 本中心共有24張ISO 27001:2013 LA、2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；3張資安職能證書。

資安服務-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），110年於8月18日、8月25日、9月2日辦理個人資管理制度教育訓練、9月9日辦理內部稽核等相關活動。

- 持續接受「教育機構資安驗證中心」稽核，以維持本校個人資料管理制度之有效性，於109年4月通過重新驗證，110年2月通過第一次追查稽核。

桃園區網提供的資安檢測(1)

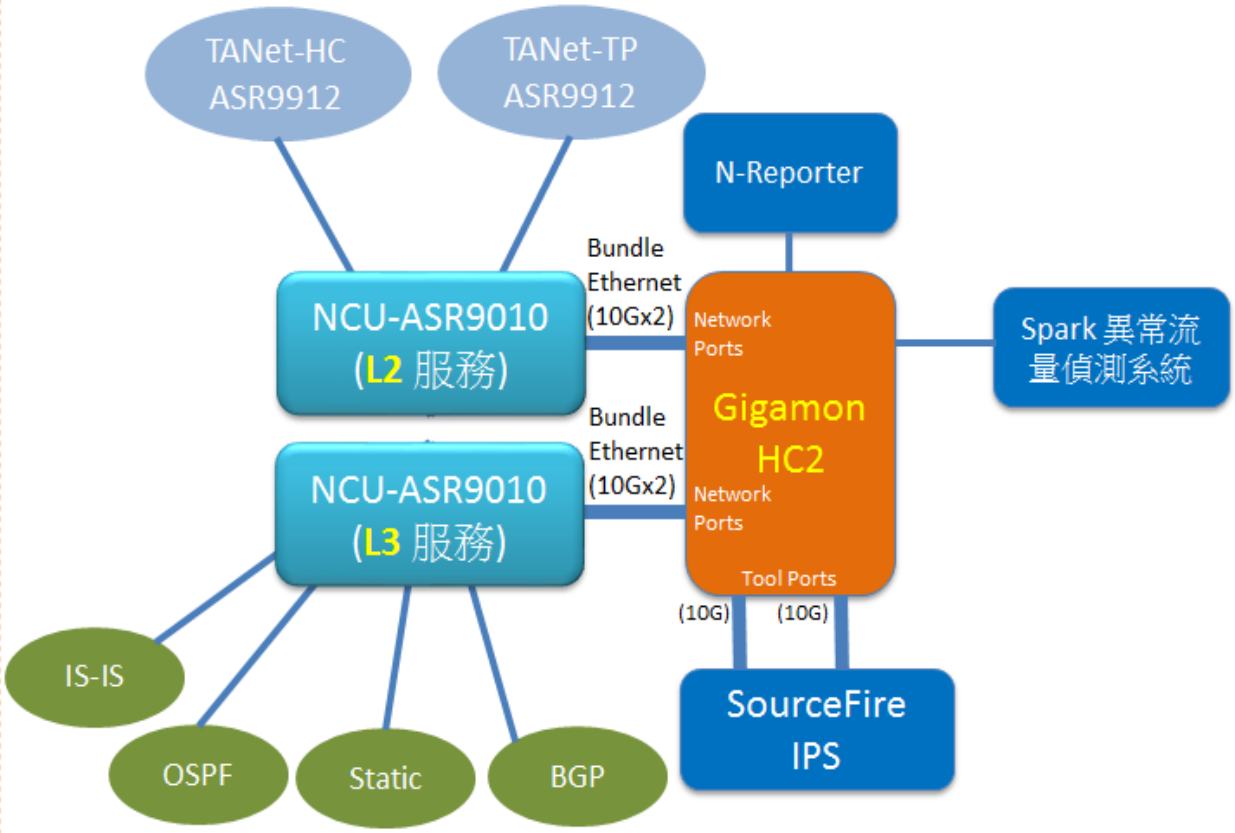
- 桃園區域網路中心每年提供2次（上半年及下半年）資安檢測服務
  - 網頁檢測（Web）使用HCL APP Scan檢測
  - 弱點掃描（IP）使用GFI LANguard(2021上半年)及Nessus（2021下半年)做為檢測工具。
- 定期追蹤申請單位是否針對弱點結果修正，修正後會再次執行掃描以確保弱點是否已修復。
- 總計協助15所學校申請弱點掃瞄 650個主機，網頁檢測 276個網站。

申請學校	弱點掃瞄	網頁檢測	追蹤處理情形
桃園市龍潭高中	2	2	2021/03/15追蹤
六和高中	3	3	2021/03/05追蹤
國立體育大學	253	230	2021/03/05追蹤
國立金門大學	10	0	2021/03/05追蹤
萬能科技大學	4	1	2021/03/16追蹤
新生醫專	1	1	2021/03/05追蹤

桃園區網提供的資安檢測(2)

申請學校	弱點掃瞄	網頁檢測	追蹤處理情形
中原大學	35	12	2021/03/10追蹤
六和高中	0	3	2021/11/3追蹤
中壢家商	3	1	2021/11/2追蹤
國立體育大學資訊中心	255	0	2021/11/5追蹤
金門縣教育網路中心	1	1	2021/11/3追蹤
中央大學電算中心	32	0	2021/11/1追蹤
至善高中	3	1	2021/11/3追蹤
中央大學總務處文書組	5	0	2021/11/1追蹤
桃園市立內壢高中	8	9	2021/11/3追蹤
中原大學	35	12	2021/11/3追蹤
總量	**650**	**276**	已全數追蹤

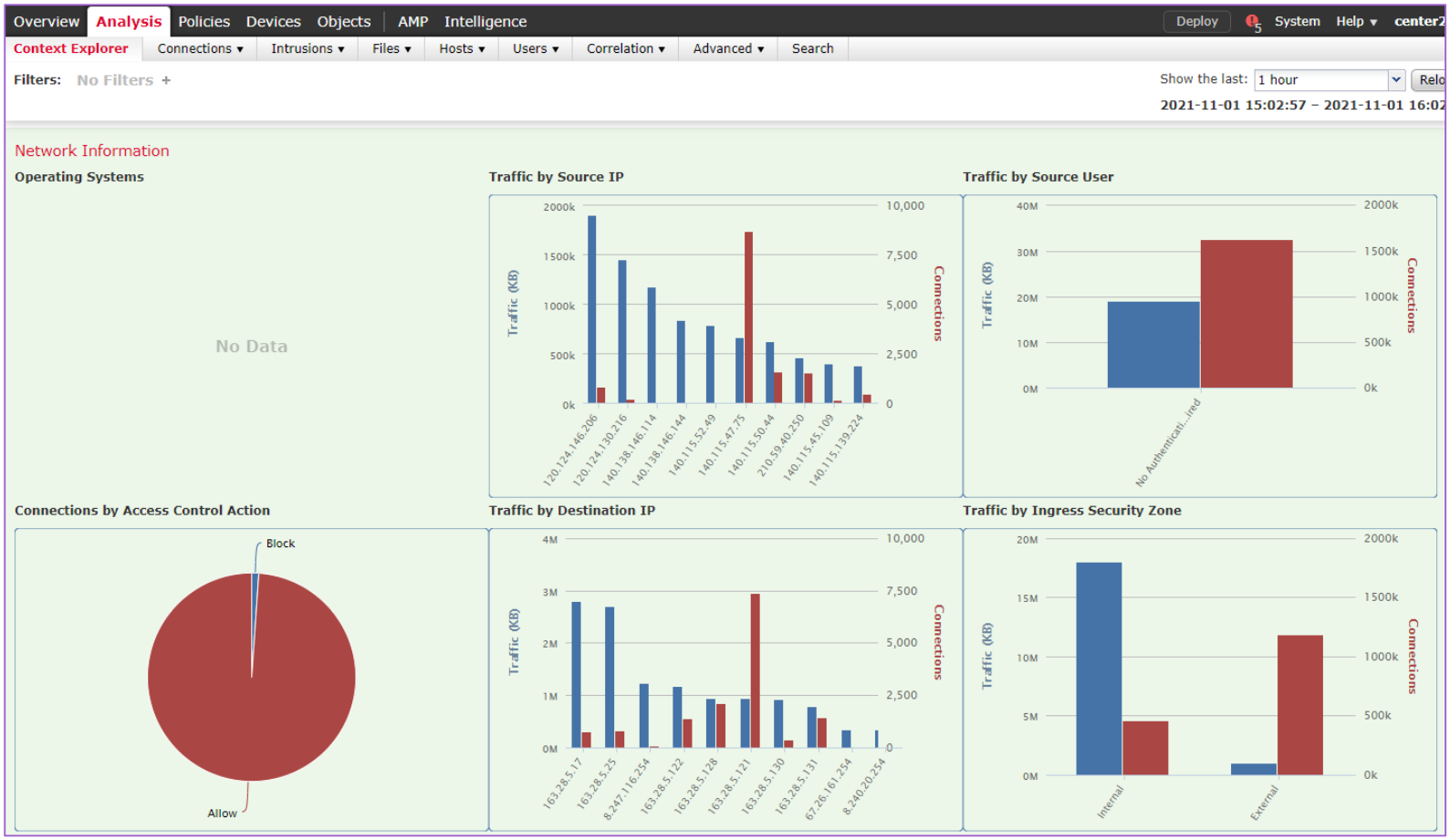
桃園區網資安系統架構



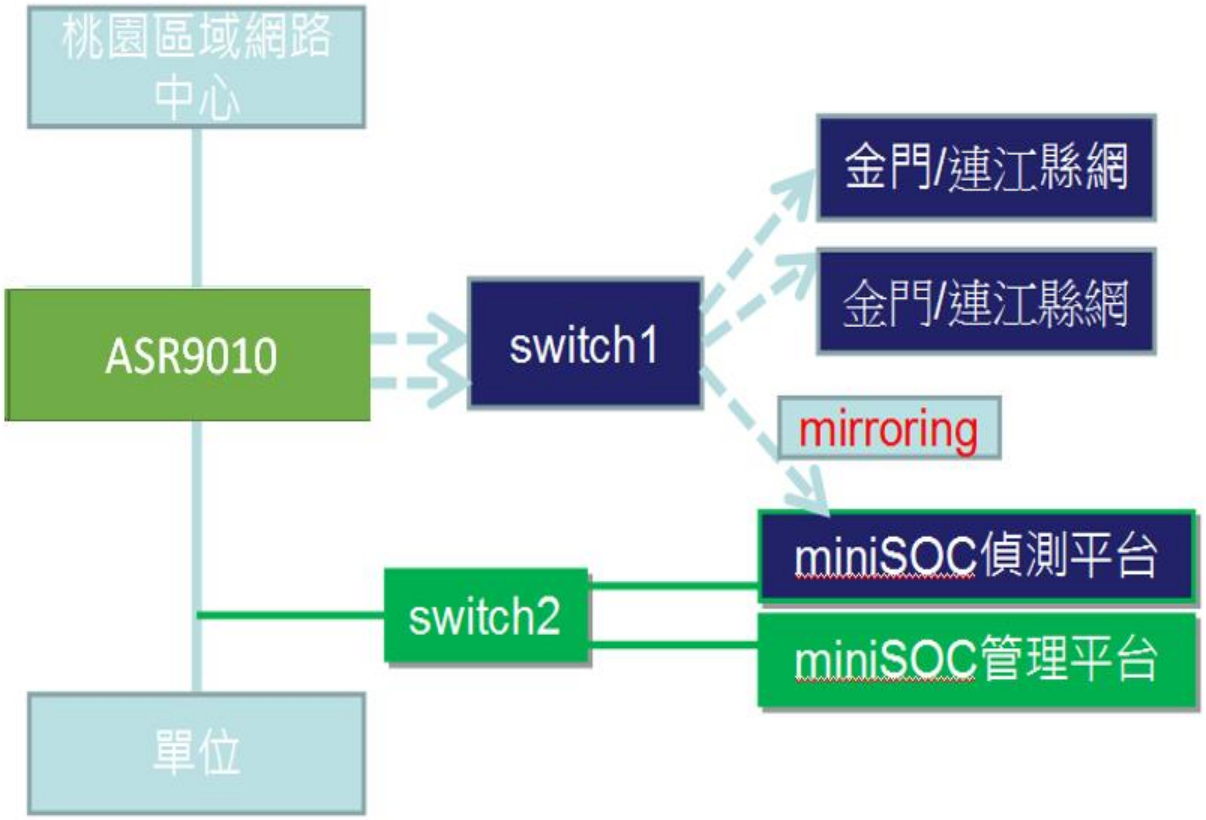
NCU-ASR9010與網路分流器架構

資安服務-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。



金門/連江MiniSOC平台



教育訓練推廣

時間	主講人	課程名稱
110年04月20日	洪嘉鴻資安顧問 台灣資訊安全聯合發展協會	駭客思維與資安攻防戰實作
110年04月29日	李美雯老師 國立臺灣大學計算機及資訊網路中心	資訊安全面面觀-從北區A-SOC維運看資訊安全
110年08月18日	洪嘉鴻資安顧問 台灣資訊安全聯合發展協會	屍戰網路-DDoS
110年08月30日	劉得民老師 中華民國網路封包分析協會理事長	勒索病毒之攻擊手法分析與案例分享
110年09月27日	張世豪講座 淡江大學	駭客攻防於IOT與公共基礎設施-基礎概念與防護

第一場-駭客思維與資安攻防戰實作

- 110年04月20日（二）
- 駭客思維與資安攻防戰實作
- 講師：洪嘉鴻資安顧問/台灣資訊安全聯合發展協會
- 上課人數：35人
- 課程大綱
  - (一)跟風
  - (二)資安教科書
  - (三)攻擊是最好的防禦
  - (四)麥當勞歡樂送
  - (五)埋伏暗殺術
  - (六)網路攻防戰
  - (七)弱者決定生死

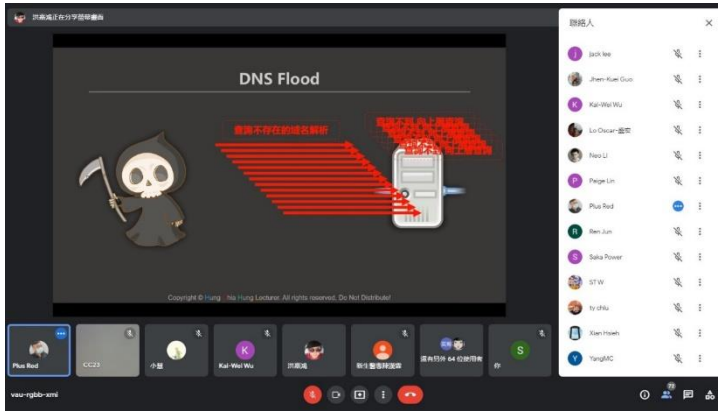
第二場-資訊安全面面觀-從北區A-SOC維運看資訊安全

- 110年04月29日（四）
- 資訊安全面面觀-從北區A-SOC維運看資訊安全
- 講師：李美雯老師/國立臺灣大學計算機及資訊網路中心
- 上課人數：32人
- 課程大綱

  此課程說明北區A-SOC如何情資偵測與分析，關於遭DDoS攻擊如何偵測與清洗流量流程。

第三場-資安防護線上講座「屍戰網路-DDoS」

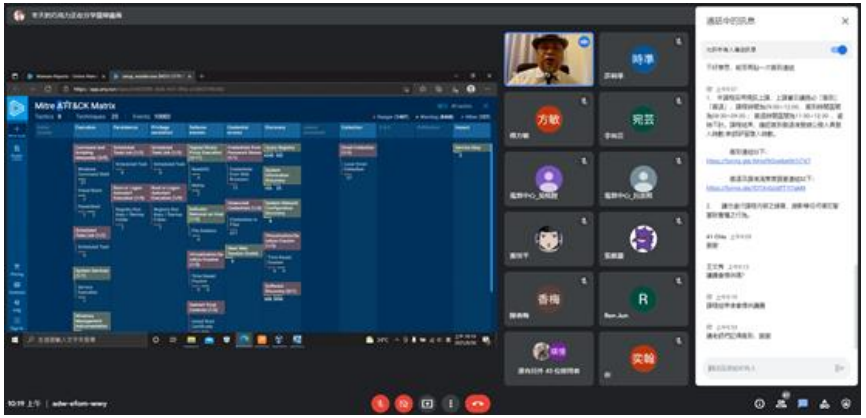
- 110年8月18日（三）
- 資安防護線上講座「屍戰網路-DDoS」
- 講師：洪嘉鴻資安顧問/台灣資訊安全聯合發展協會
- 上課人數：66人
  （疫情影響，採線上視訊）



- 課程大綱
  （一）資安趨勢
  （二）駭客思維
  （三）DDoS技術
  （四）惡意流量分析
  （五）DDoS演練<實作>
  （六）資安防護
  （七）資安意識

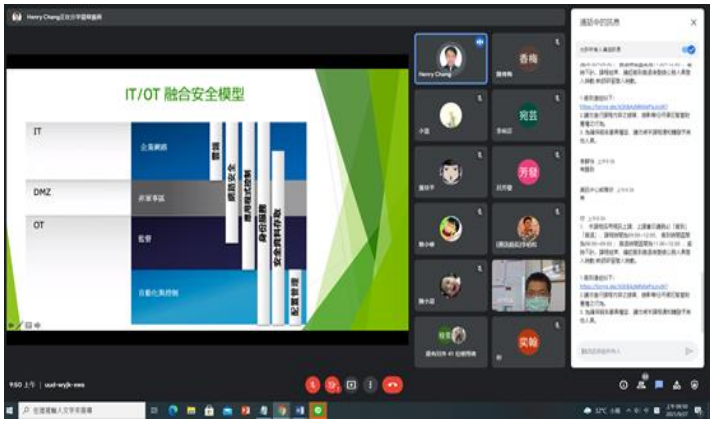
第四場-勒索病毒之攻擊手法分析與案例分享

- 110年08月30日（一）
- 講師：劉得民老師 /中華民國網路封包分析協會理事長
- 上課人數：49人
- 課程大綱
  1. 加密勒索攻擊的基本要素
  2. 加密勒索攻擊的途徑
  3. 前常見加密勒索種類
  4. 加密勒索攻擊範例
  5. 如何防範加密勒索



第五場-駭客攻防於IOT與公共基礎設施

- 110年09月27日（一）
- 駭客攻防於IOT與公共基礎設施-基礎概念與防護
- 講師：張世豪講座/淡江大學
- 上課人數：47人
- 課程大綱
  1. 資訊科技安全與威脅介紹
  2. 常見的駭客攻擊類型
  3. 物聯網介紹
  4. 物聯網安全技術
  5. 認識關鍵資訊基礎設施資安
  6. 關鍵資訊基礎設施防護



預計年底前教育訓練

- 第六場：11月24日 善用全球智慧—自建同步視訊系統
- 講師：辛文義組長/新竹縣教育研究發展暨網路中心
- 課程大綱：介紹運用Open Source 的 Bigbluebutton來打造的校園視訊直播服務。
  (1)軟硬體環境準備
  (2)架構部署視訊直播服務
  (3)實務維運上遭遇的挑戰
  (4)擴展提升雲服務效能
  (5)教育訓練與推廣規劃
  (6)創新應用和未來發展

- 第七場：12月16日 Windows 及 Linux 主機架設安全防護

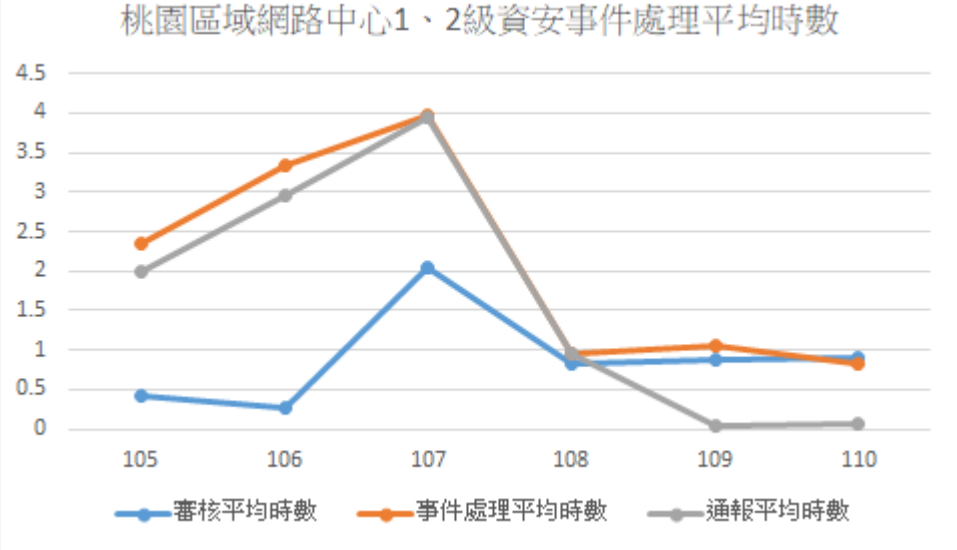
重大營運事件之檢討

- 本年度桃園區網中心無重大營運(網管及資安)事件。

資安事件統計

資料統計：2021/1/1-2021/09/30		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	0.06
(2)應變處理平均時數：	小時	0.03
(3)事件處理平均時數：	小時	0.85
(4)通報完成率：	百分比	100%
(5)事件完成率：	百分比	100%
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	0.96
聯絡相關資訊完整度：	百分比	100%

歷年資安事件處理平均時數



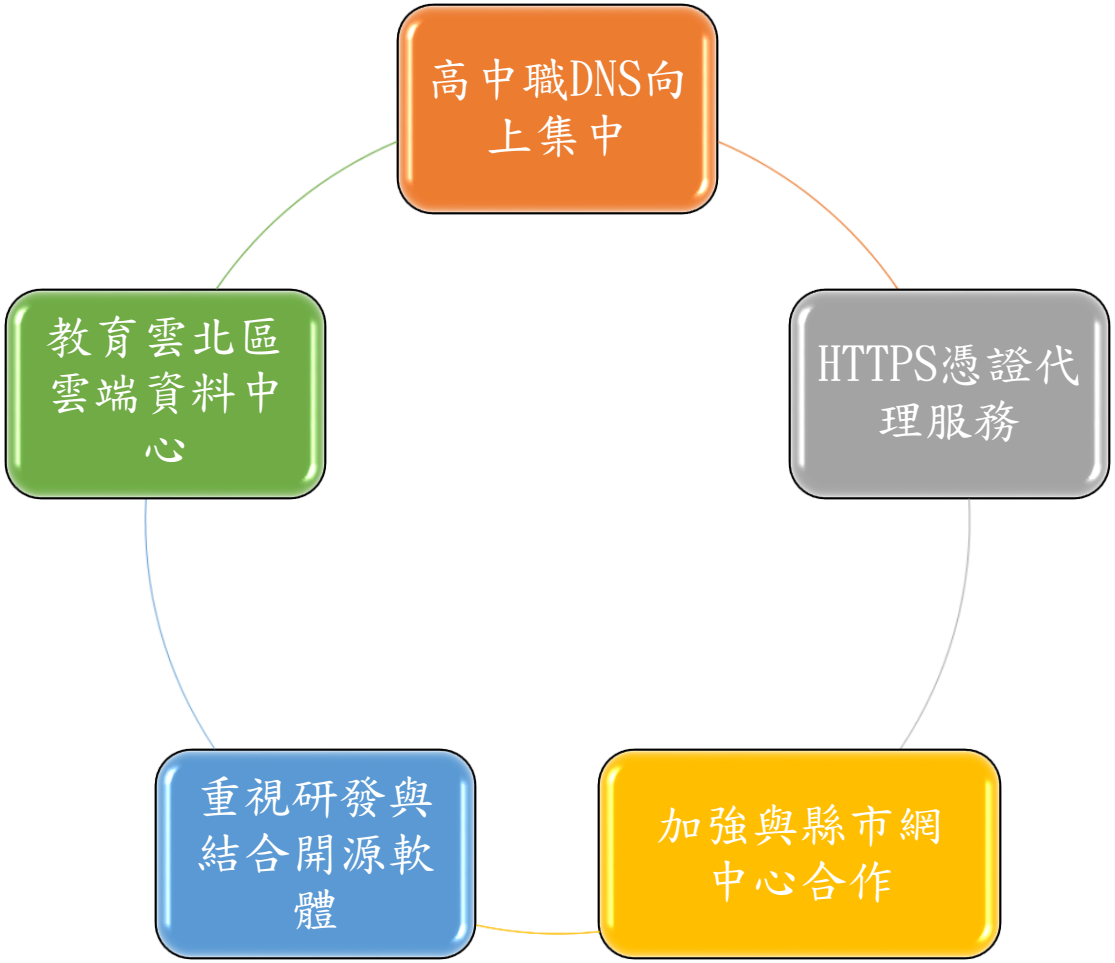
年度	105	106	107	108	109	110
審核平均時數	0.41	0.28	2.04	0.829	0.87	0.96
事件處理平均時數	2.34	3.34	3.98	0.961	1.05	0.85
通報平均時數	2	2.97	3.95	0.96	0.05	0.06

第四章

國立中央大學

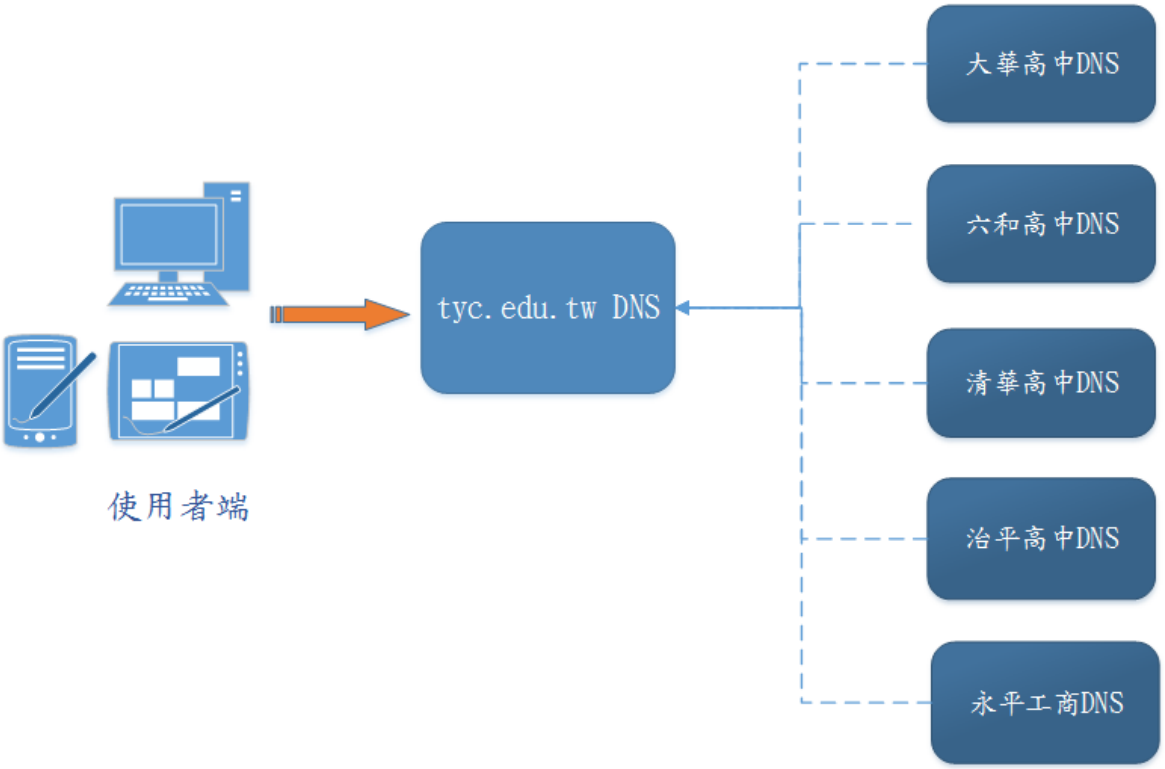
特色服務

特色服務


高中職DNS向上集中
HTTPS憑證代理服務
加強與縣市網中心合作
重視研發與結合開源軟體
教育雲北區雲端資料中心

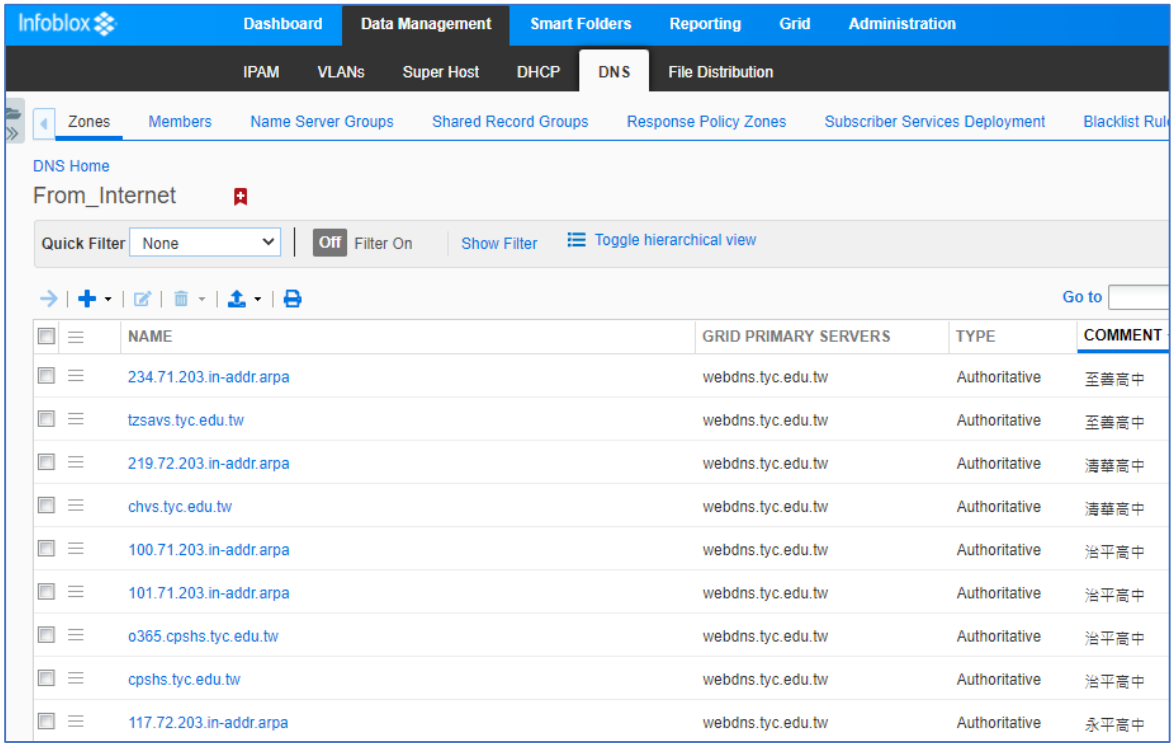
高中職DNS 向上集中(1)

- 2021年桃園區網中心與桃園市網中心合作
- 主動協助私立高中職學校DNS伺服器向上集中，累計至10月底完成11所私立高中職DNS向上集中。



高中職DNS 向上集中(2)

- DNS向上集中優點
  - 減少學校建置管理DNS系統維護成本。
  - 完成DNSSEC簽署及RPZ設定，增加了DNS服務安全性。
  - 達成環保節能減碳，減少11所學校共13台 DNS 伺服器的能源消耗。



高中職DNS 向上集中(3)

- 前置作業中已先將11所學校 bind record，以人工方式逐一轉換至新系統匯入格式，資料必須依不同類型轉換成符合新系統之格式，筆數近800筆。並事先於測試主機測試正常後，始能於約定日迅速轉換(10分鐘內完成)，縮短對作業學校網路服務之影響。

序	學校	DNS集中完成日期
1	大華高中 thsh	110/07/30
2	六和高中 lhvs	110/08/10
3	清華高中 chvs	110/08/16
4	振聲高中 fxsh	110/08/17
5	治平高中 cpshs	110/08/19
6	復旦高中 fdhs	110/08/30

序	學校	DNS集中完成日期
7	永平工商 ypvs	110/08/31
8	新興高中 hshs	110/08/31
9	啟英高中 cyvs	110/08/31
10	至善高中 tzsavs	110/08/31
11	大興高中 dxhs	110/10/13

HTTPS 憑證代理服務(1)

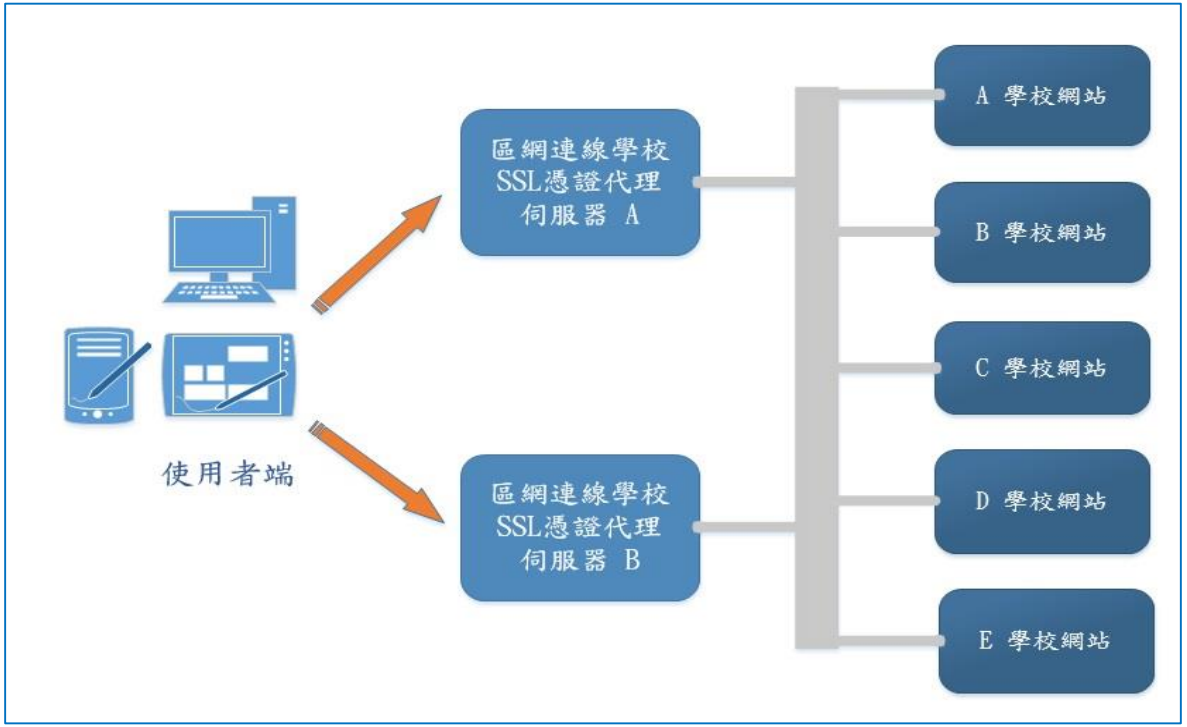
- 教育部110年6月29日臺灣學術網路(TANet)技術小組第96次會議決議，各級學校網站應導入 HTTPS。

- 桃園區網協助連線學校導入HTTPS過程中，大專院校有比高中職較多的人力與資源，而公立國高中學校有市網中心協助，但私立高中職學校網站升級 HTTPS有其困難度，原因如下:

  - 部分私立高中職資訊經費拮据，硬體平台使用多年，機器老舊。
  - 學校資訊組長一人負責全校所有網路及資訊工作，工作繁重，網站及應用系統無廠商維護。

HTTPS 憑證代理服務(2)

- 桃園區網中心利用開源軟體NGINX的反向代理特性，達成後端網站伺服器的SSL憑證代理。
- 累計至10月底完成7所學校，共15個學校網站導入HTTPS。



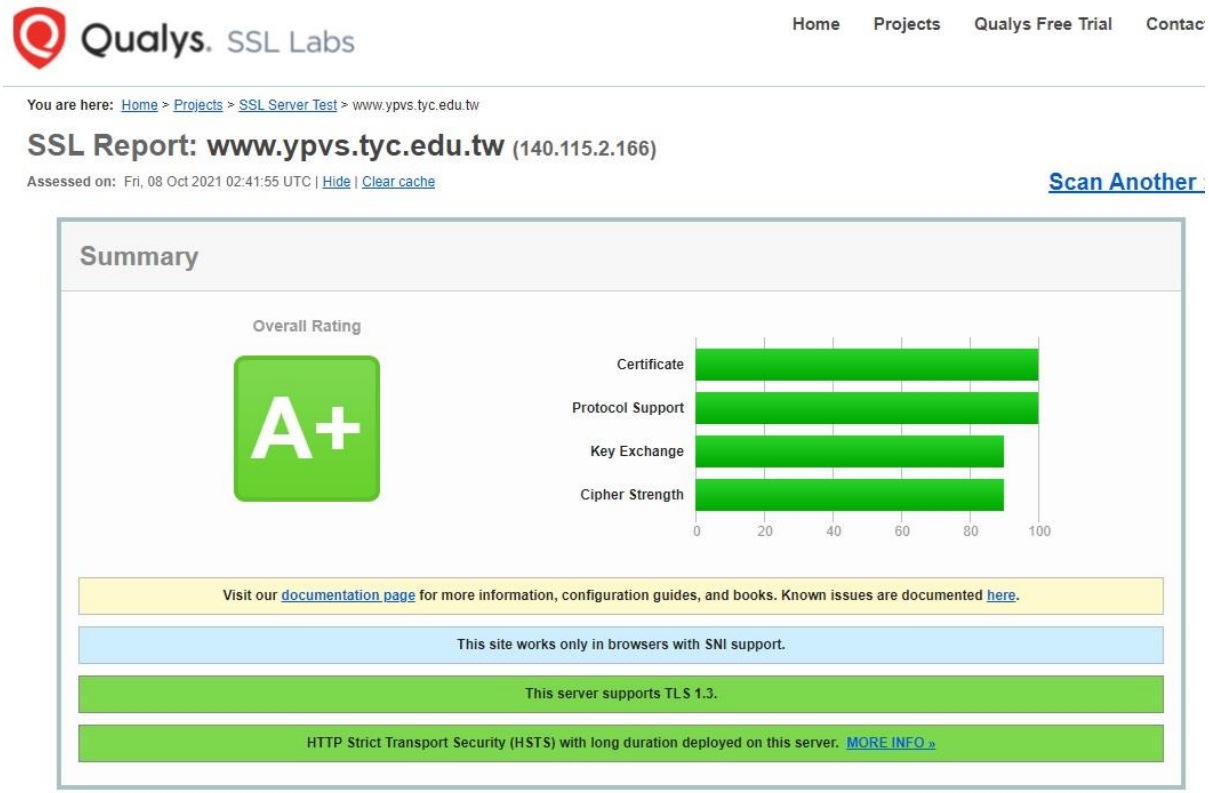
論文發表於TANET2021研討會

HTTPS 憑證代理服務(3)

- 26% 的學校網站在完全不需要更動原網站設定及網站程式碼下，順利導入HTTPS 。
- 74% 的學校網站也能在區網協助下，變動幅度甚小之後完成導入HTTPS。
- 變動部分由桃園區網中心與學校資訊組長共同檢視網頁混合內容，以相對連結 URL 取代絕對連結 URL。
- 修改網站設定及調整網站程式以導入HTTPS。

HTTPS 憑證代理服務(4)

- 憑證代理使用TLSv1.2，TLSv1.3，以及HSTS（HTTP Strict Transport Security），讓瀏覽器瀏覽網站時，強制使用HTTPS進行連線傳輸。
- 協助連線學校網站取得A+ 安全性評等。



HTTPS 憑證代理服務(5)

序	學校	HTTPS 憑證代理 完成日期
1	大華高中 thsh	110/08/11
2	振聲高中 fxsh	110/08/19
3	永平工商 ypvs	110/08/30
4	啟英高中 cyvs	110/09/01
5	成功工商 ckvs	110/09/24
6	復旦高中 fdhs	110/10/05
7	大興高中 dxhs	110/10/14

加強與縣市網中心合作

- 本年度與桃園市網中心合作，協助11所私立高中職學校DNS伺服器向上集中，達成提升DNS安全性及減少人力維護成本，並同時完成DNSSEC簽署及RPZ設定。

- 本年度與金門縣網中心合作，在金門縣網人力編制有限及人事異動的狀況下，針對其需求進行手把手的實作教學，辦理資訊安全管理系統導入、機房管理訪視與網路巡檢。

ISMS導入實作、資產盤點、風險評鑑

- 協助金門縣網中心ISMS導入實作，建立ISMS推動組織、建立四階文件。
- 依照實際資產清單進行資產盤點、風險評鑑。

機房管理、網路巡檢

- 協助金門縣網中心機房管理，包含檢視機房設備安全維護，機房冷氣、電力、不斷電系統管理狀態。

- 網路巡檢包含網路架構檢視，網路區隔管理及存取控制措施，光纖或易遭受破壞之線路保護措施。

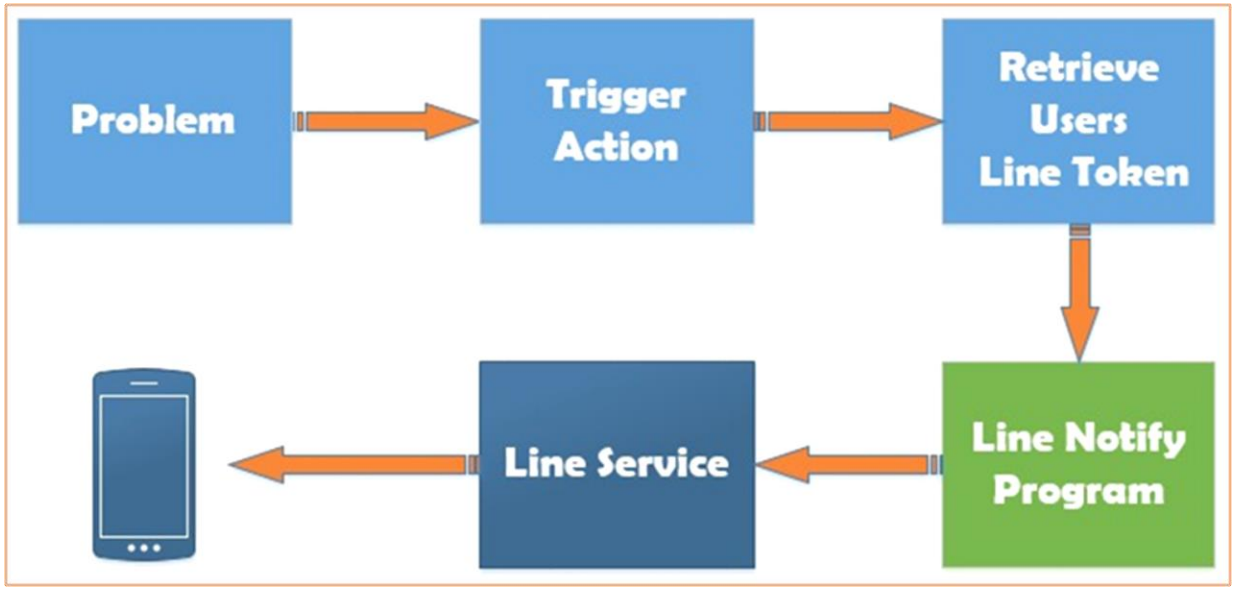
重視研發與結合開源軟體(1)

- 桃園區網面對網路管理以及資安的各項需求，試著以開源軟體為基礎，並結合自行開發的程式以完成各項任務，並將這些經驗投稿至TANET研討會。

研討會名稱	論 文 題 目	備 註
TANET2021研討會	SSL憑證代理伺服器之建立與導入-以桃園區網中心為例	
TANET2020研討會	自動監測系統結合LINE 即時訊息通知-以桃園區網中心為例	最佳人氣論文獎
TANET2019研討會	Open Source Security Onion 系統之導入與應用-以桃園區網中心為例	
TANET2018研討會	Open Source SIEM系統之導入與應用 -以桃園區網中心為例	佳作論文獎
TANET2017研討會	以網路分流器彈性部署入侵偵測與防禦系統-以桃園區網中心為例	
TANET2016研討會	自動化調整雲端Spark異常流量偵測系統	
TANET2015研討會	結合 Spark 與 Hadoop於雲端平台進行網路異常流量偵測	

重視研發與結合開源軟體(2)

- 2020年桃園區網中心透過導入開源Zabbix系統，監測重要網路設備、機房溫溼度，以確保網路及機房設備全年無休的正常運作。
- 區網中心並自行開發LINE Notify程式，即時發送LINE Notify訊息，讓網管人員隨時掌控機房環境及網路服務是否正常運作。



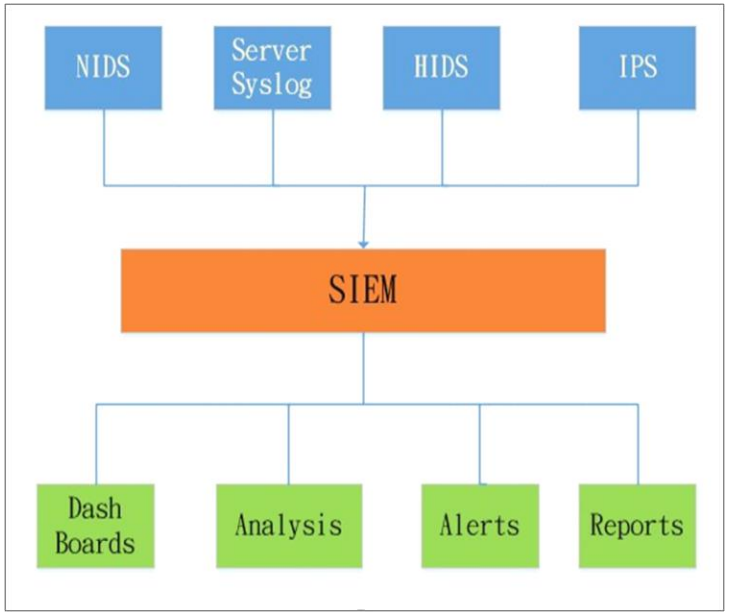
TANET2020研討會最佳人氣論文獎

重視研發與結合開源軟體(3)

- 2018年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。

- 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。

60



TANET2018研討會佳作論文獎

重視研發與結合開源軟體(4)

- 2015年自行開發Spark異常流量偵測系統，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中快速找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。

TANET2015研討會論文

教育雲北區雲端資料中心

- 提供的資源
  - CPU: 216 vCPU (108 core)
  - RAM: 1504 GB
  - HD: 可用 70TB (鏡像的備份)
- 使用的軟體
  - 雲端管理軟體
    - VMware
  - 虛擬化儲存軟體

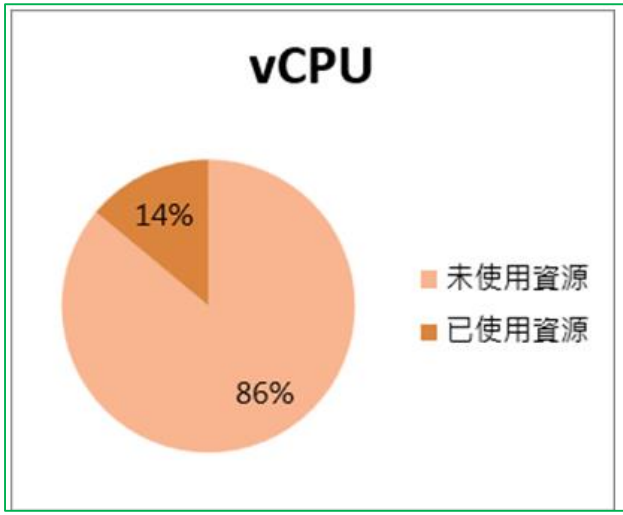
教育雲上的服務系統詳細資源

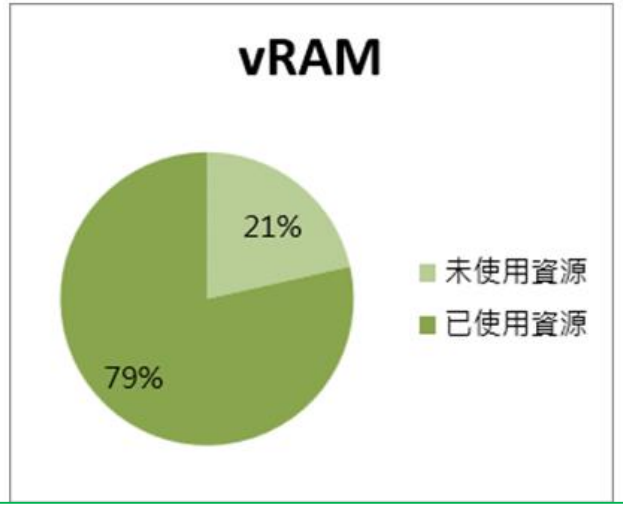
服務系統名稱	vm數量	vCPU	vRAM	vHD
TANet_VoIP	3	12	48	240
中華開放教育平台	11	48	152	24519
因材網	9	124	304	3600
字音字形網	1	8	16	160
英語線上學習平台	2	24	96	3050
教育單位弱點檢測平台	1	8	16	100
教育媒體影音	6	24	48	9117
教育體系單一帳號驗證授權平臺	10	80	208	950
教師研習平台	4	32	64	3589
微積分題庫	1	4	8	100
數學小學堂系統	3	14	28	1301
體育署_體育雲-全民運動資訊系統	13	60	120	3956
體育署_體育雲-全民運動資訊系統報名網站	9	40	80	900
體育署_體育資訊雲端	3	12	24	300
總計	**76**	**490**	**1212 (GB)**	**50.66(TB)**

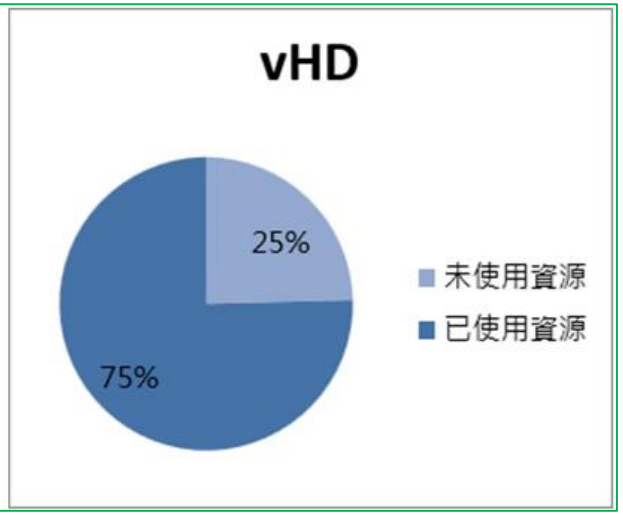
教育雲北區雲端資料中心—資源使用情況

項目	*vCPU	vRAM (GB)	vHD(TB)
總資源量	216	1504	70
未使用資源	185.87	322.75	17.21
已使用量	30.13	1181.25	52.79
已使用量(%)	13.95%	78.54%	75.41%

*32 Virtual CPUs per core







國立中央大學

未來營運方針與創新服務目標

未來營運方針

- 持續機房維運建設(電力、空調)，維持良好網路運作，完成所有學校導入IPv6 環境。
- 提供連線學校網路實體環境資安防護機制及資安檢測服務。
- 加強與縣市網中心合作，並持續與金門及連江縣網中心合作機房管理與網路巡檢。
- 加強雲端服務，提供建置私有雲及教育雲服務之經驗分享與推廣。
- 持續推動以開源軟體為基礎，結合自行開發程式以完成任務。

成立桃園區網中心資安關懷團隊

接獲轄下各連線單位之請求協助通知時，視需要派員到校參與協助應變處理

提供資安改善建議，以增進各連線單位資安防禦能量

＊ 團隊成員擁有證照: 5張ISO27001、2張CHFI、1張CEH、1張CISSP證照

＊ 預計2022年培訓成員參加 EC-Council ECIH資安危機處理員認證課程

資安關懷團隊作業程序

＊ 連線單位發生重要主機資安事件

↓

＊ 協助進行緊急應變處理

↓

＊ 協助進行損害管制作業

↓

＊ 協助後續資安改善建議

提供資安改善建議

協助評估資訊安全防護機制

協助評估資料備份機制

協助評估災難復原機制

第五章

國立中央大學

成效精進

執行成效精進情形(1)

項次	109年度委員建議	改進及精進做法
1	IPv6之建置推動已經多年了，建議明年是否能協助將大專校院部分先完成，高中職及其他單位分兩年來完成，將此項業務告一段落。	今年大專院校已全數完成導入IPv6。高中職部分今年已完成4所導入，並有2所高中導入中。預計2022年完成所有連線學校導入IPv6環境。
2	人員工作穩定在職提供服務，其薪資及勞健保等應可事先預估費用，建議在規劃下年度計畫預算時，能更精確預估人事費以使繳回教育部之經費能更低(雖然目前已經不高)。	遵照委員指示辦理，109年計畫執行率已達99.99%以上。
3	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，通報及應變處理成效佳，惟事件處理平均時數建議可再加強。	透過區網會議宣導及LINE群組聯繫，事件處理平均時數已由109年的1.05小時，降低到110年的0.85小時。

執行成效精進情形(2)

項次	109年度委員建議	改進及精進做法
4	DNS 版本更新，請清查尚有多少學校未完成，盡速協助完成。	大專院校部分，已全數更新至最新版本，高中職部分，也透過DNS向上集中解決。
5	明年之KPI 值設定較保守，建議可再調高，來自我挑戰。	遵照委員指示辦理，原訂定今年KPI協助至少1所連線學校導入IPv6，最後完成4所學校導入，並有2所進行中。
6	教育訓練的部分可以強化在實務能力提升的指標設定與達成。	今年教育訓練的課後問卷中，對於【是否符合實務學習需要?】選項，填答【非常滿意】的比率為77 %，未來將以達到【非常滿意】80%為訓練成效指標。
7	在資安防護技術提升的教育訓練可以強化上線練習的課程。	今年有4堂提供實務操作的練習，惟受限疫情，無法進行面對面的實機指導練習，未來疫情稍緩，將以開設實機上線練習為目標。

執行成效精進情形(3)

項次	109年度委員建議	改進及精進做法
8	雖已協助轄下連線單位導入ipv6，但尚有諸多學校 DNS 尚未支援 IPv6，去年(108)已有委員建議可規劃在本年度完成連線學校 IPv6 之建置，惟仍未見具體成效，另外針對連線單位 DNS 版本老舊之問題，建議應加強了解並協助處理。	大專院校部分，DNS已全數更新至最新版本並支援IPv6，高中職部分也透過DNS向上集中逐步解決。
9	109年計劃書仍有許多篇幅沿稱教育部電算中心，計劃書內容應再務求精確。	遵照委員指示辦理，計畫書已全數修正完畢。
10	因應資安法導入及資訊資源向上集中政策，請評估協助區網連線高中職學校DNS及主機虛擬化代管的可行性。	遵照委員指示辦理，本年度與桃園市網合作，協助11所私立高中職DNS向上集中。
11	建議日後赴所轄離島縣市網路中心(連江、金門)，可評估協助巡檢網路及機房環境向上集中。	遵照委員指示辦理，本年度10月22日赴金門縣網中心辦理ISMS導入及機房管理、網路巡檢等工作。

KPI績效指標執行情形

110年KPI指標執行率

項次	110年度 KPI指標說明	執行情形
1	全年電路服務妥善率：99.9 %以上。	本年度無斷線紀錄
2	召開 2 次區域網路中心管理會議，邀請4個連線單位分享該校網路管理經驗。	100%
3	辦理 7 場網路管理及資訊安全教育訓練，其中至少 4 場資安及網管訓練實作課程， 參與人次達 200 人次。	預估100% (已辦理5次，超過220人次，年底前將再辦理2場訓練)
4	協助至少 9 所連線學校進行弱點掃描、網站網頁檢測等資安服務。	100%（已協助15所學校）
5	協助至少 3 所連線學校導入 IPv6 ，並完成桃園區網所有連線大專院校導入IPv6。	100%（已協助4所學校，另2所進行中）
6	每年至一個離島縣市教育網路中心提供網管資安研習、巡檢網路機房環境或技術支援服務。	100%
7	提供至少 2 所連線學校到校資安研習或網管及資安之技術支援服務。	100%，受限新冠肺炎疫情，本年度暫停提供到校研習等服務，惟今年仍以遠端協助7所高中網站導入HTTPS服務。

111年KPI指標

項次	111年度 KPI指標說明
1	全年電路服務妥善率：99.9 %以上。
2	召開 2 次區域網路中心管理會議，邀請4個連線單位分享該校網路管理經驗。
3	辦理 7 場網路管理及資訊安全教育訓練，參與人次達200人次，並達到【非常滿意】80%為訓練成效指標。
4	協助至少 7 所連線學校進行弱點掃描、網站網頁檢測等資安服務。
5	協助至少 4 所連線學校導入 IPv6。
6	每年至一個離島縣市教育網路中心提供機房環境管理及巡檢網路及技術支援服務。

綜合建議

- 協助高中職教育相關系統全面統一並向上集中管理
- ISP電路太過昂貴，希望大專院校也可以有折扣

2021

國立中央大學

National Central University

許時準組長
center20@cc.ncu.edu.tw