臺灣學術網路TANet 竹苗區域網路中心HCRC

111年度區域網路中心
年終成果報告

竹苗區域網路中心 國立陽明交通大學 資訊技術服務中心

報告人 高義智 組長

111年11月18日

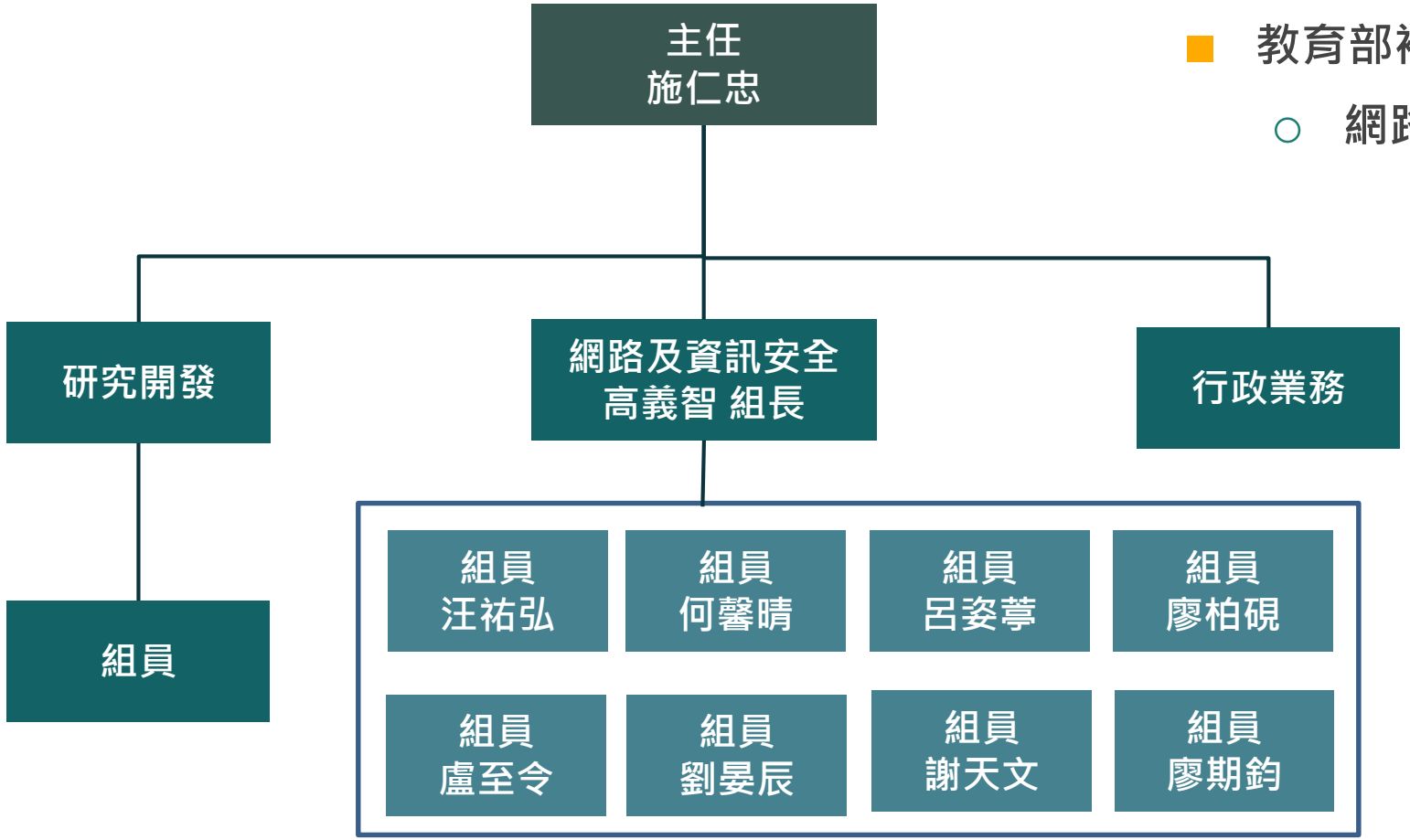
大 綱

1. 經費及人資運用
2. 基本資料及運作情形
3. 服務導入與活動辦理
4. 網路維運管理服務
5. 資通安全管理與應用
6. 應用創新服務
7. 111年度計畫績效指標辦理情形
8. 112年度預計推動之重點工作

1. 經費及人資運用

組織架構

- 專職與兼任參與維運所投入人力：10人
- 教育部補助款專職人員：2人
  - 網路維運１人、資安雲端１人



人員證照

類型	證照	人數	合計
網路類	Cisco Certified Internetwork Expert(CCIE)	1	6
	Cisco Certified Network Professional(CCNP)	2	
	Cisco Certified Network Associate(CCNA)	3	
資安類	ISO-27001	7	22
	ISO-27701	2	
	The CREST Practitioner Security Analyst (CPSA)	1	
	EC-Council ECSA	1	
	Computer Hacking Forensic Investigator(CHFI)	2	
	Certified Ethical Hacker(CEH)	2	
	CCSK(Certificate of cloud security knowledge v4)	2	
	資安職能證書	5	
管理類	Project Management Professionnal(PMP)	1	1

教育部支援網管及資安人力運用

- 教育部補助款專職人員：2人（網路維運１人、資安及雲端１人）

網管維運人員工作執掌

- **TANet竹苗區網網路維運**
  - 維護HiNet CDN 竹苗區網營運點
  - 維護竹苗區網與 ISP 業者 BGP peering
  - 維運骨幹網路
  - 維運網路監控系統
  - 維護虛擬主機系統
  - 維護網頁公告平台
  - 維護DNS server
- **協助連線單位建置服務**
  - 建置單位內網管系統
  - 建立IPv6網路環境
  - 導入eduroam無線網路漫遊服務

資安及雲端人員工作執掌

- **協助連線單位資安業務**
  - ISO27001稽核
  - 教育機構防洩漏個資掃描平台維護及審查
  - 處理教育部資安通報
  - 處理竹苗區網中心資安事件
  - 辦理資通系統安全檢測服務
- **協助雲端管理**
  - 協助各單位進行教育部資安通報演練
  - TANet設備資訊機房管理
- **辦理教育訓練**
  - 舉辦教育訓練課程

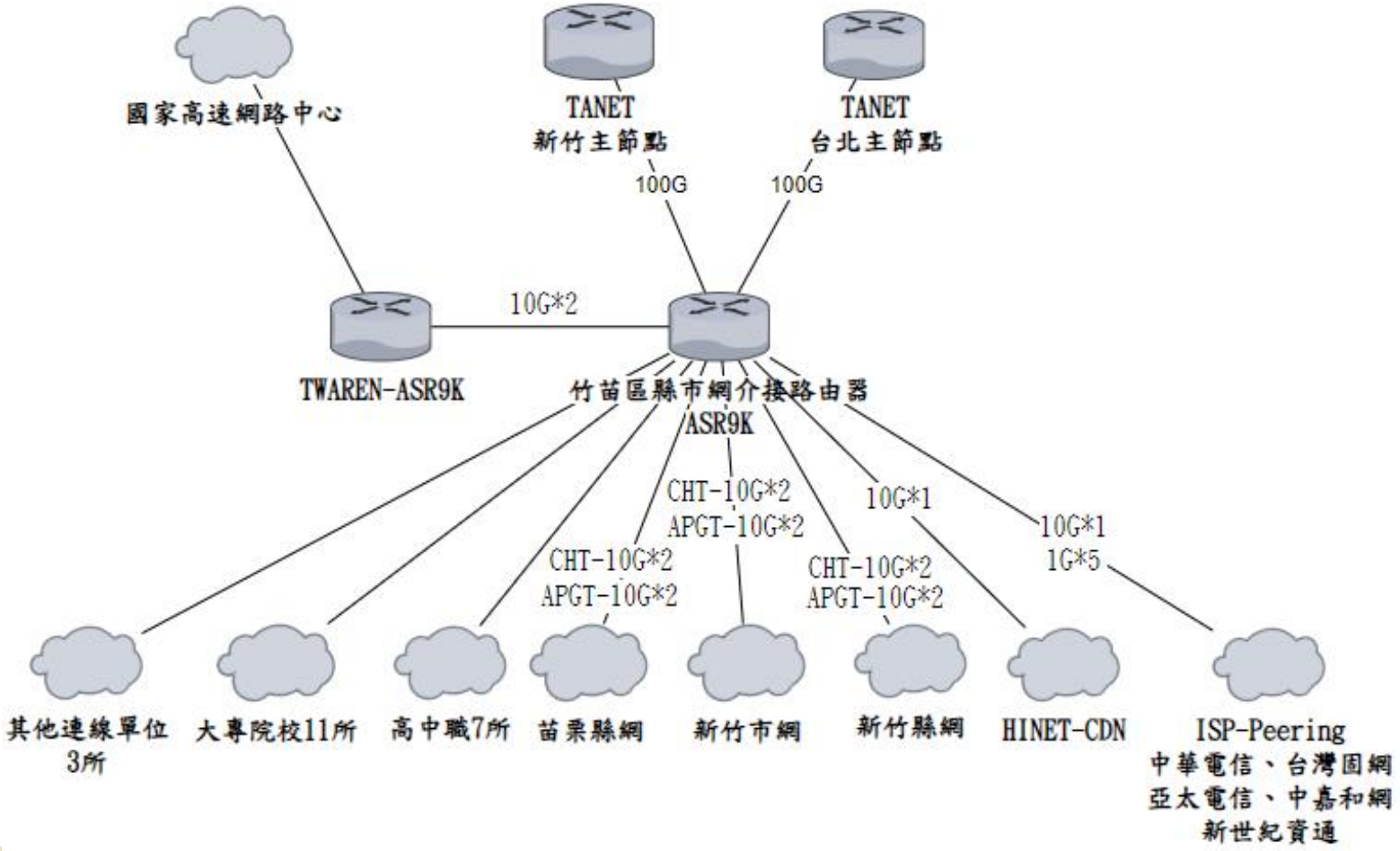
竹苗區網中心經費運用情形

經費來源	經費項目	經費編列	使用比率	備註說明
教育部補助款 1,570,000	人事費	1,268,368	83%	資安維運人力
	業務費	151,632	78%	教育訓練、雜支
	設備費	150,000	100%	網路設備及記憶體擴充
		總執行率	83%	累計至10月，預計於12月可達95%以上。

2. 基本資料及運作情形

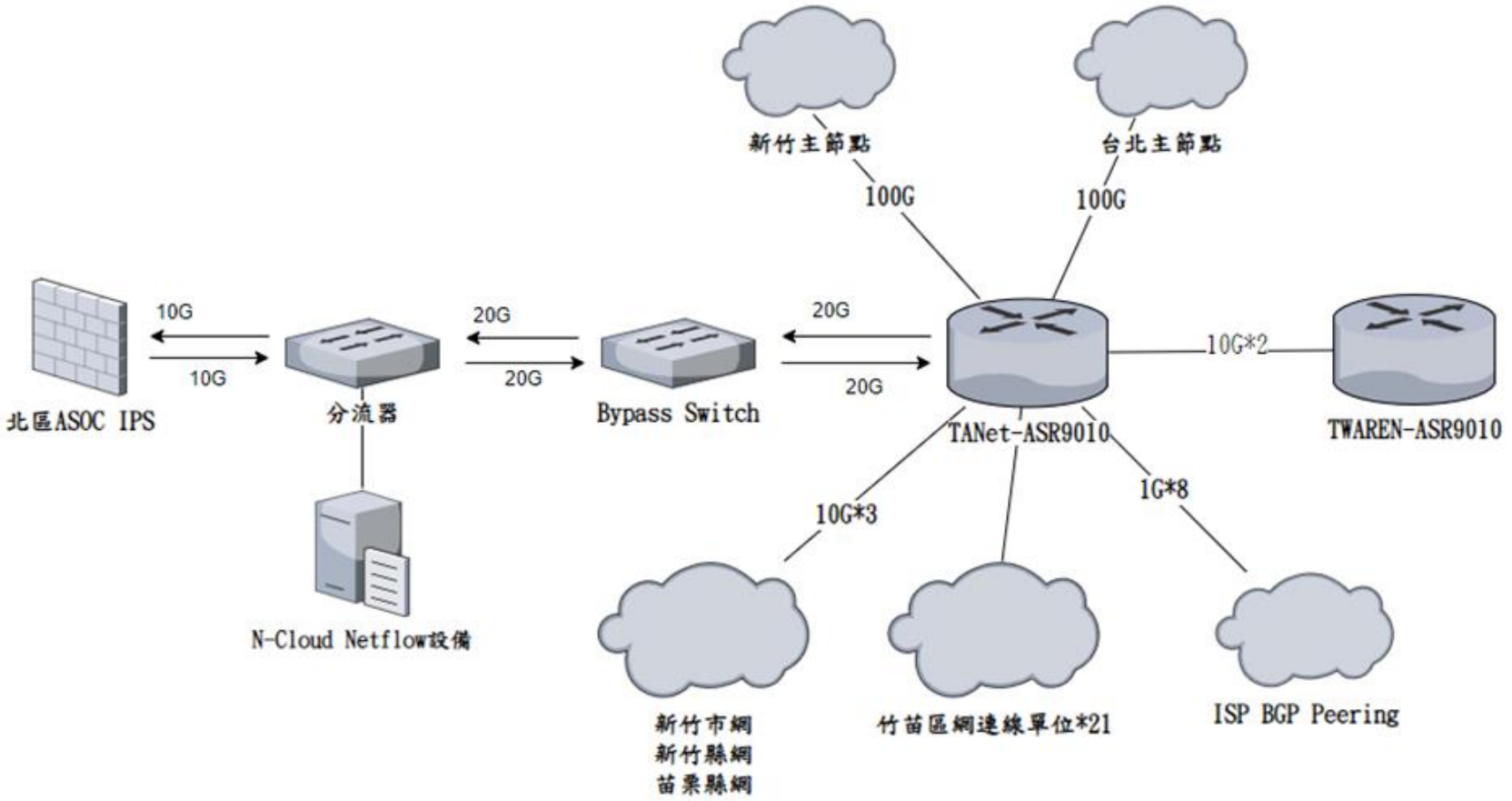
竹苗區網網路拓撲

- 111年竹苗區網網路拓撲圖 https://www.hcrc.edu.tw/structure/



竹苗區網網路拓撲

- 111年竹苗區網資安架構拓撲圖 https://www.hcrc.edu.tw/structure/



區網連線單位

- 竹苗區域網路中心共 24 所連線單位。

縣(市)網中心	大專院校	高中職	研究機關
• 新竹市教育網路中心 • 新竹縣教育網路中心 • 苗栗縣教育網路中心	• 陽明交通大學 • 聯合大學 • 玄奘大學 • 中華大學 • 元培科技大學 • 育達科技大學 • 明新科技大學 • 敏實科技大學 • 仁德醫專 • 中華科技大學(新竹分部) • 中國科技大學(新竹分部)	• 新竹高中 • 新竹高商 • 曙光女中 • 世界高中 • 實驗高中 • 光復中學 • 忠信高中	• 食品工業研究所 • 台灣半導體研究中心 • 新竹縣文化局
3	11	7	3

連線單位類別及頻寬統計

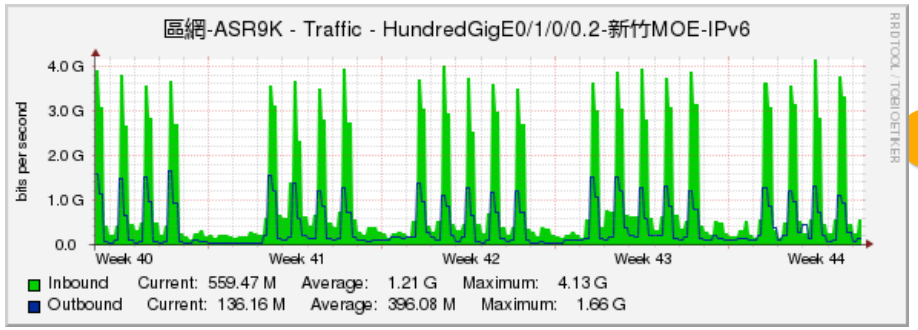
111年竹苗區網連線單位類別及頻寬統計

- 頻寬1G以上單位達 58%，100M~1G達38%，100M以下4%。
- 苗栗縣網中心因網路設備無10G模組，暫時無法進行升級。已規劃於112年度進行模組擴充。

頻寬＼單位	縣(市)網中心	大專院校	高中職	研究機關	合計
20G	3	-	-	-	3
10G	-	2	-	-	2
1G~<2G	-	5	4	1	10
100M~<300M	-	4	2	2	8
100M以下	-	-	1	-	1
合計	3	11	7	3	24

3. 網路服務導入與活動辦理

連線單位IPv6服務



TANet HCRC

- 連線單位已 **100%** 全數導入IPv6服務，並對外連線使用。

連線單位	IPv6
新竹市教育網路中心	2001:288:4200::/48
新竹縣教育網路中心	2001:288:4400::/48
苗栗縣教育網路中心	2001:288:4600::/48
國立陽明交通大學	2001:288:4001::/48
聯合大學	2001:288:4002::/48
玄奘大學	2001:288:4006::/48
中華大學	2001:288:4004::/48
元培科技大學	2001:288:4008::/48
育達科技大學	2001:288:4009::/48
明新科技大學	2001:288:4005::/48
敏實科技大學	2001:288:4007::/48
仁德醫專	2001:288:4019::/48

連線單位	IPv6
中華科技大學(新竹分部)	2001:288:400C::/48
中國科技大學(新竹分部)	2001:288:400B::/48
新竹高中	2001:288:4010::/48
新竹高商	2001:288:4016::/48
曙光女中	2001:288:400F::/48
世界高中	2001:288:4013::/48
實驗高中	2001:288:4015::/48
光復中學	2001:288:4012::/48
忠信高中	2001:288:4014::/48
食品工業研究所	2001:288:4018::/48
台灣半導體研究中心	2001:288:4017::/48
新竹縣文化局	2001:288:401B::/48

無線網路eduroam服務

- **連線單位導入eduroam無線服務**
  - 111年度已完成4所單位，共累計16所單位導入，導入率達 **66%**。
  - 尚未導入單位多為技術能量不足、設備不支援，將持續協助單位推動導入服務，今年已邀請漫遊中心單位進行教育訓練。

已導入單位	
新竹市教育網路中心	元培科技大學
新竹縣教育網路中心	玄奘大學
苗栗縣教育網路中心	新竹高中
陽明交通大學	新竹高商
聯合大學	曙光女中
明新科技大學	光復高中
育達科技大學(111年度)	**世界高中(111年度)**
敏實科技大學(111年度)	**實驗高中(111年度)**

辦理管理委員會情形

- 本年度召開竹苗區網管理委員會2次，出席率平均達 **83.8%**。
  - 因部分人員為教師身分，課程時間常與委員會相衝，於會後皆提供內部錄影檔供人員參考。

83.8% 期中出席率

111年度第一次管委會　111年5月27日

- 網站弱點檢測服務說明
- 區網中心NetFlow設備更新事宜
- TANet DNS 遞迴查詢服務

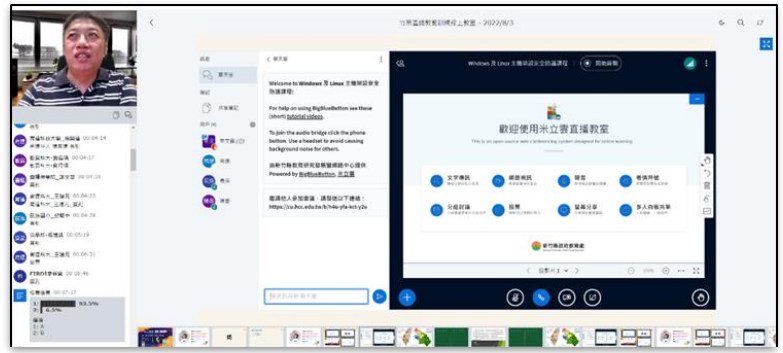
83.8% 期末出席率

111年度第二次管委會 111年10月26日

- EVS平台網站弱點掃描
- 系統主機弱點掃描服務申請
- 滿意度調查

辦理教育訓練及推廣活動情形

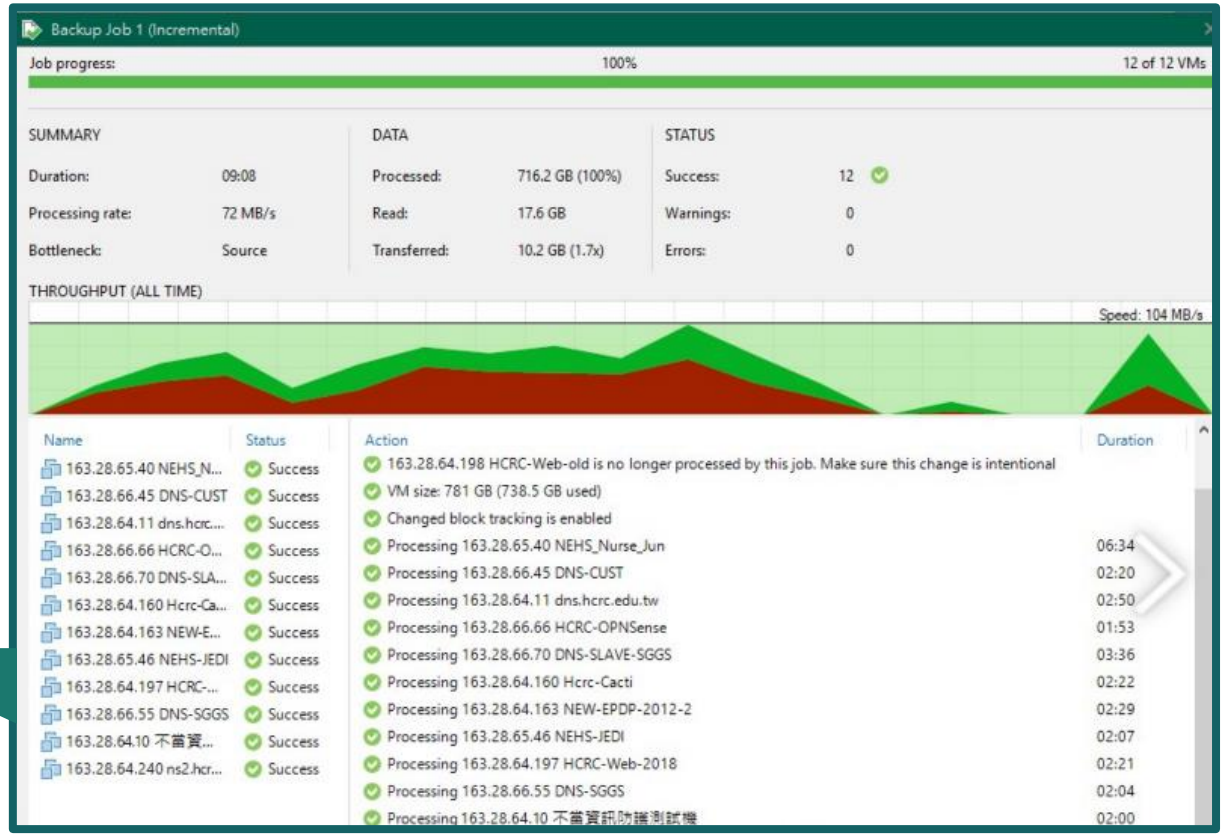
- 本年度舉辦連線單位網管人員訓練 6 場次(3H/場)
  - ○ 邀請業界、其他縣市網中心及學校之人員進行交流分享，類型包含資訊安全、網路資訊及系統服務課程，累積人次達243位。

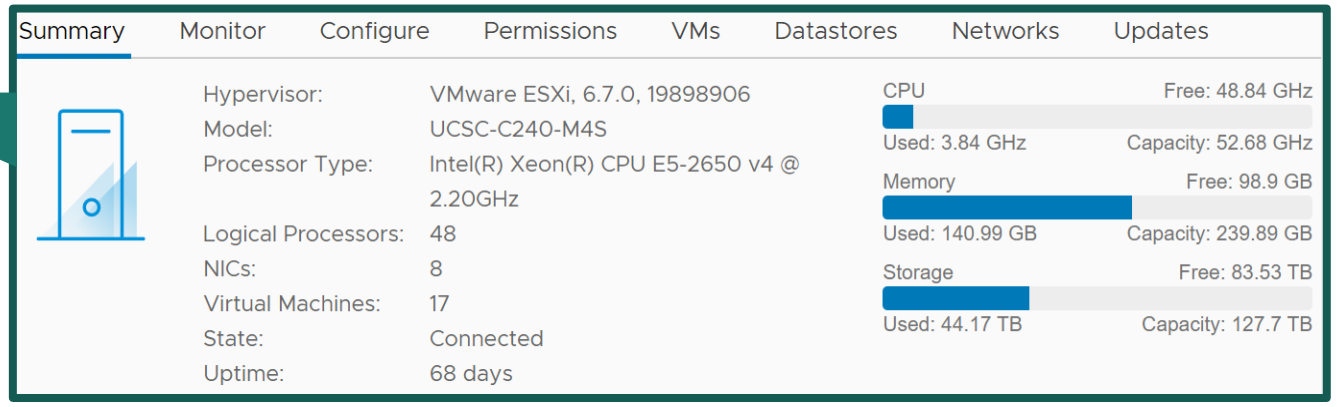


111年5月27日	111年7月13日	111年8月3日	111年8月10日	111年8月17日	111年10月26日
eduroam無線網路漫遊導入說明	資訊安全面面觀─從北區A-SOC維運看資訊安全	善用全球智慧─自建同步視訊系統	校園網路管理的藝術─The Dude	N-Cloud 6.0實務教學與應用	資通安全實地稽核之因應分享
35人	37人	49人	52人	35人	35人

系統虛擬化服務

- **提供連線單位申請虛擬主機**
  - 已協助7所連線單位進行建置，共建置36台虛擬機。
- **系統主機備份服務**
  - 提供建置於區網虛擬機內的系統主機進行備份。
- **強化硬體資源效能**
  - 今年度購入記憶體，提升虛擬機硬體效能。





4. 網路維運管理服務

機房營運節能配置

採冷熱通道配置

- 機房內通道採冷熱方式建置，降低能源使用。
- 夏日電力使用效率：1.64
- 冬日電力使用效率：1.6

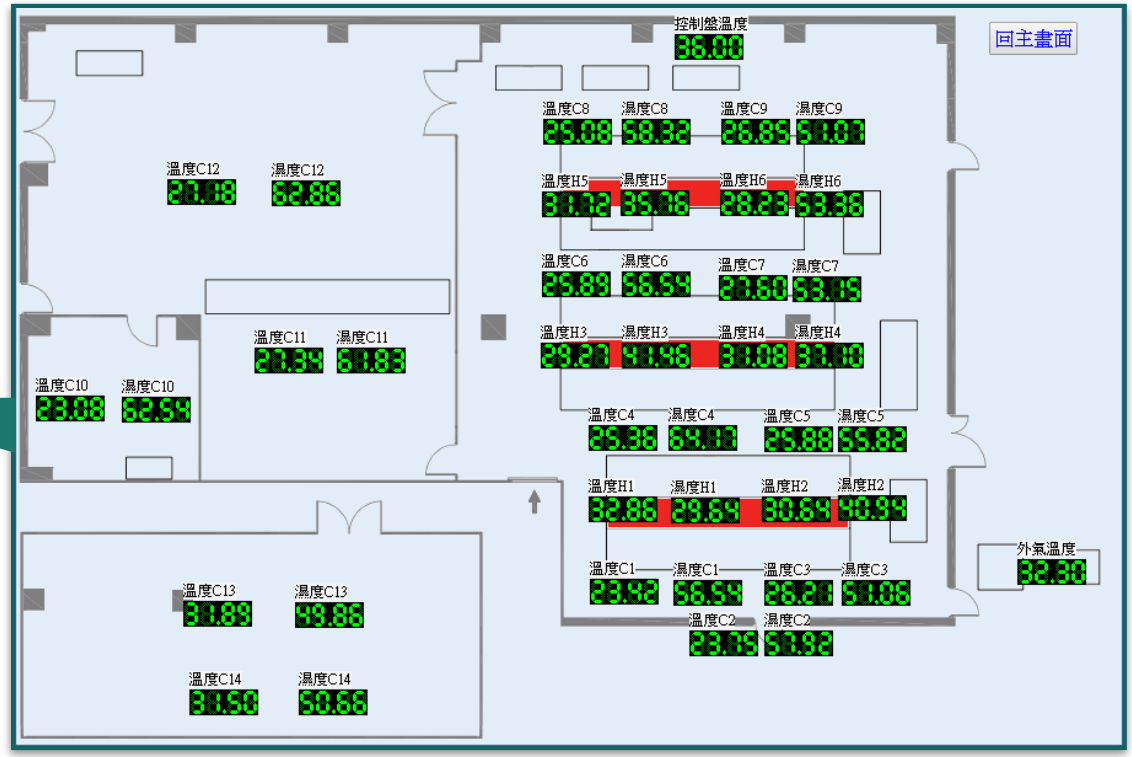
結構化分區佈線

- 將光纖線路與網路相關設備進行分區，僅針對設備區域進行降溫，以節約能源。

機房環境監控管理

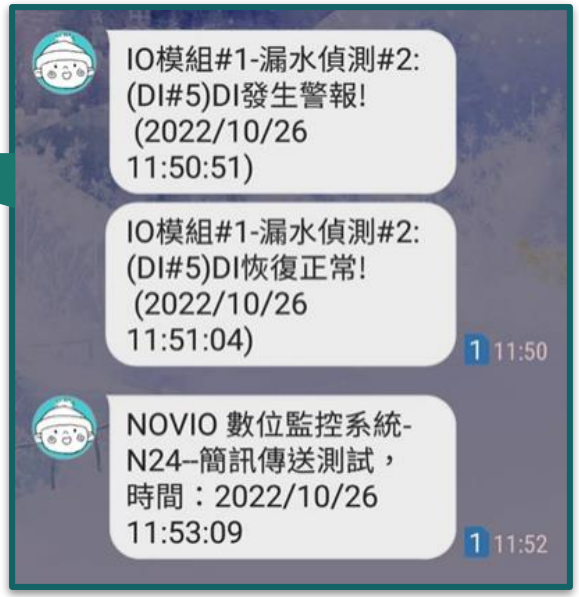
即時了解機房運作

- 本中心建置環控系統，機房管理員可24小時監控機房狀態，如電力、空調、溫濕度等參數。



即時告警機制

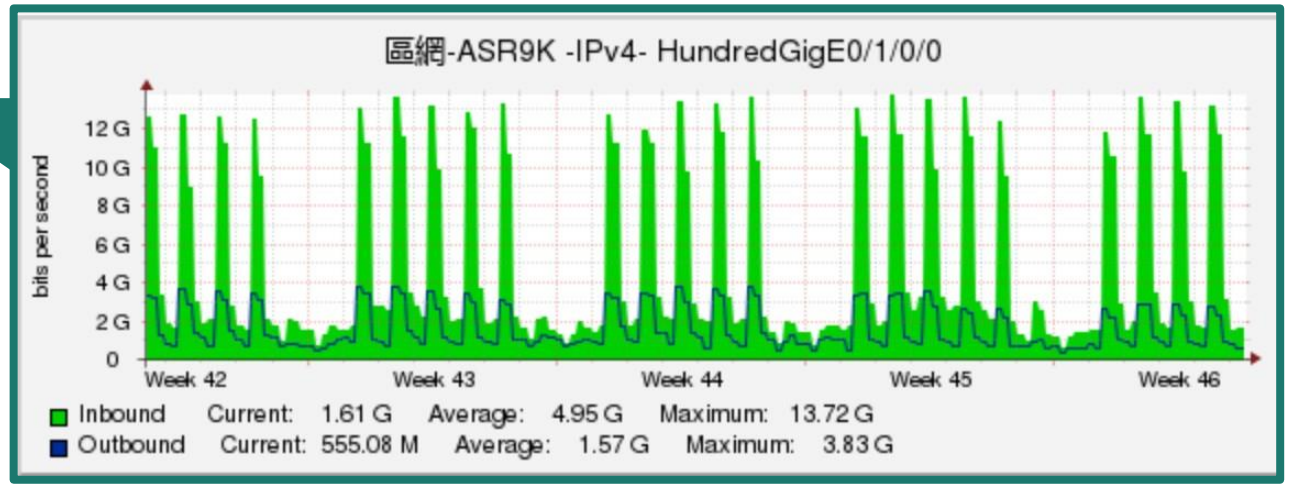
- 若發生異常狀況，如溫溼度超標，系統將即時寄發通知告知網管人員。



網站流量監控可用率

骨幹網路可用率

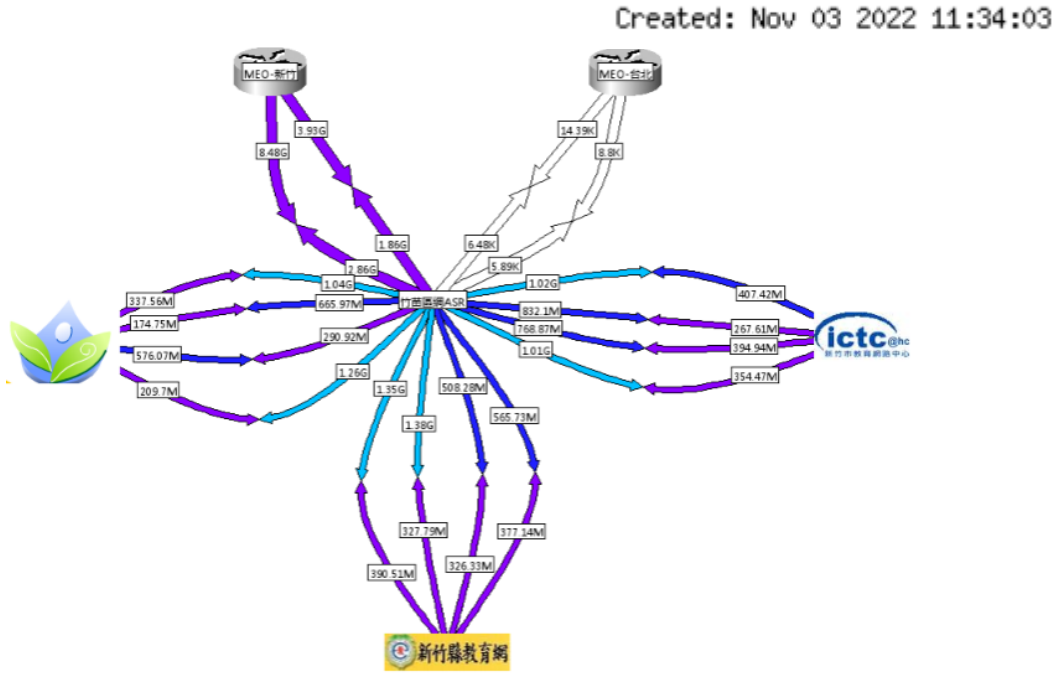
- 今年度竹苗區網骨幹網路可用率達 **99.99%**。
- 區網中心透過監控系統程式進行流量監控，以供網路管理人員掌握即時的流量資訊。若發生線路異常或是頻寬接近滿載之情形，將會發送告警告知管理人員。

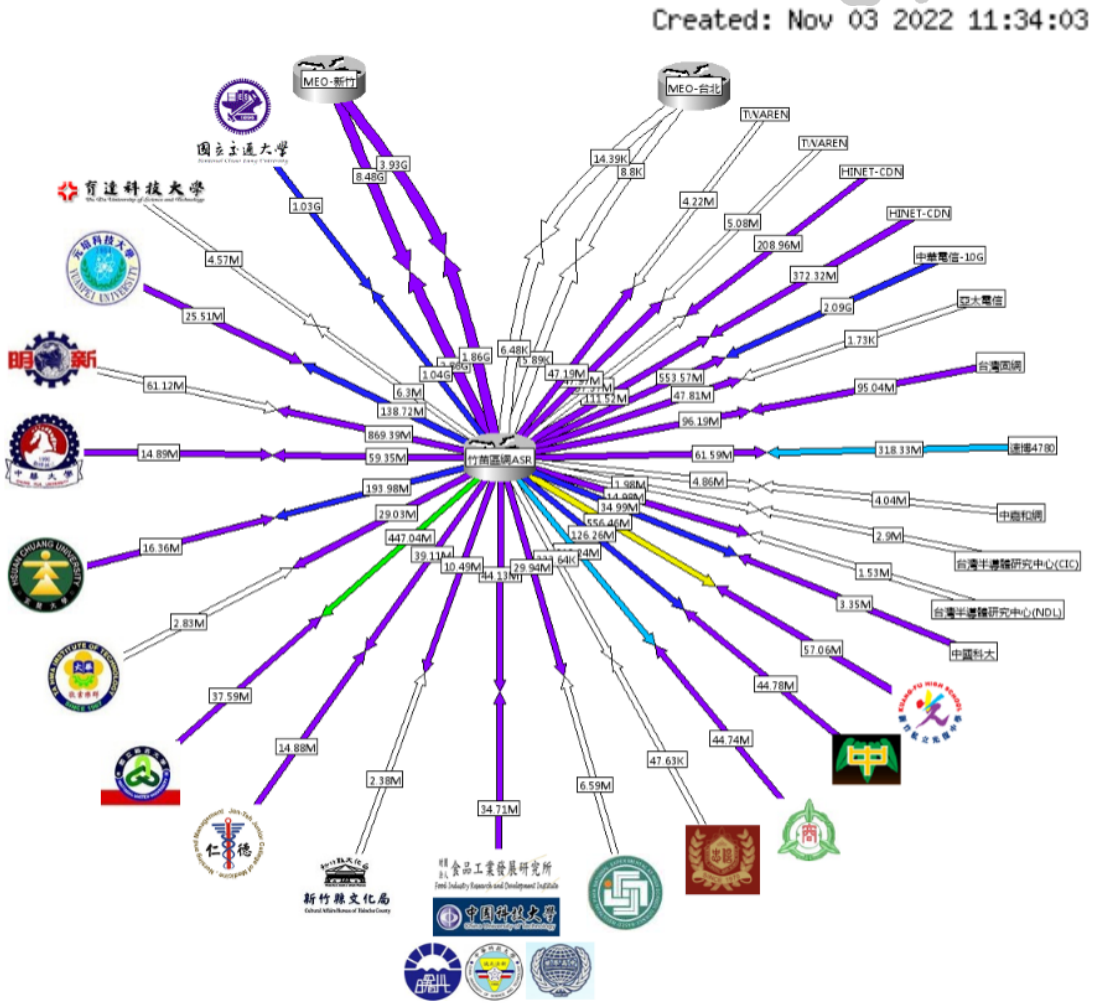


網路流量即時監控

- 提供連線單位即時監控網路流量查詢
  - Cacti網路即時流量：

    https://www.hcrc.edu.tw/graph/





網路流量紀錄分析

TANet HCRC

- **專屬單位帳號查詢流量紀錄分析結果**
  - 開啟25個領域及所屬帳號，提供連線學校自行查詢分析自單位Netflow。

操作	報表名稱
	HCRC-中國科技大學新竹分部下載流量圖
	HCRC-中華大學下載流量圖
	HCRC-亞太創意技術學院下載流量圖
	HCRC-元培科大下載流量圖
	HCRC-國家晶片系統設計中心下載流量圖
	HCRC-國家奈米元件實驗室下載流量圖
	HCRC-國立竹北高級中學下載流量圖
	HCRC-大華科大下載流量圖
	HCRC-新竹市世界高中下載流量圖
	HCRC-新竹市光復高中下載流量圖
	HCRC-新竹市新竹高中下載流量圖
	HCRC-新竹市新竹高商下載流量圖

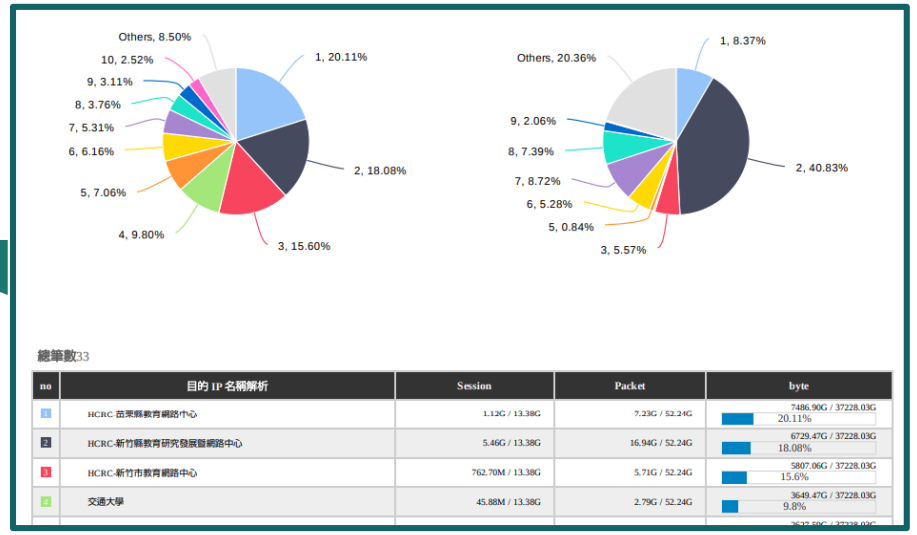
- **建置多種分析監控報表**
  - 已於系統內建立43個TopN報表、35個分時監控報表。

No.	目的名稱解析	Sessions	Packets	Bytes
1	HCRC-苗栗縣教育網路中心	1.12G	7.23G	7486.90G
2	HCRC-新竹縣教育研究發展暨網路中心	5.46G	16.94G	6729.47G
3	HCRC-新竹市教育網路中心	762.70M	5.71G	5807.06G
4	交通大學	45.88M	2.79G	3649.47G
5	HCRC-新竹市光復高中	114.73M	2.20G	2627.59G
6	HCRC-明新科大	723.82M	2.77G	2293.38G

網路流量紀錄報表

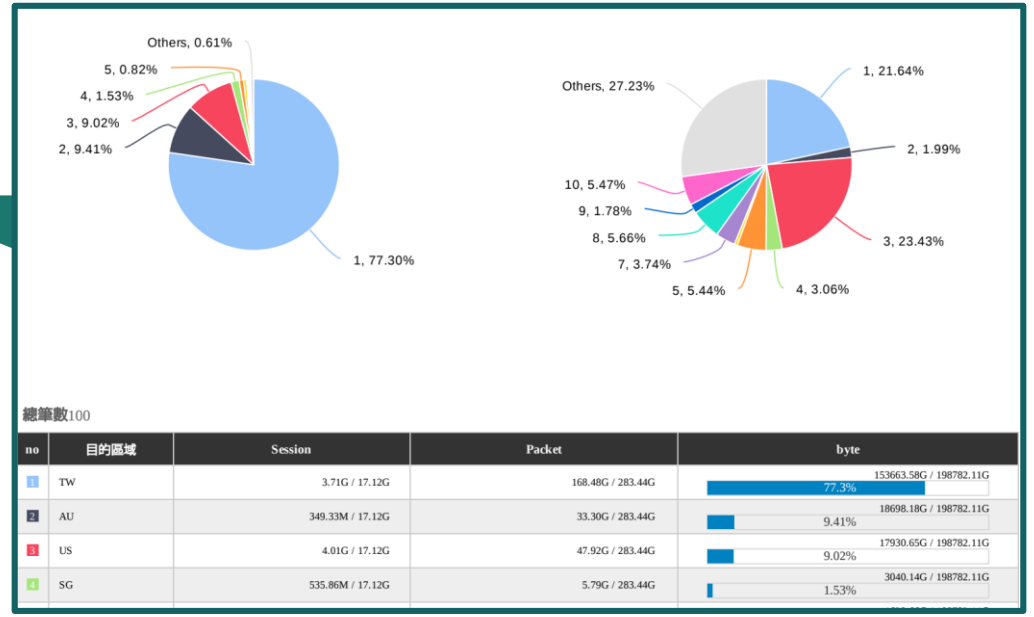
連線單位下載用量排名統計

- 每週統計區網各連線單位的網路下載量，並寄發給單位網管老師。



連線國家排名統計

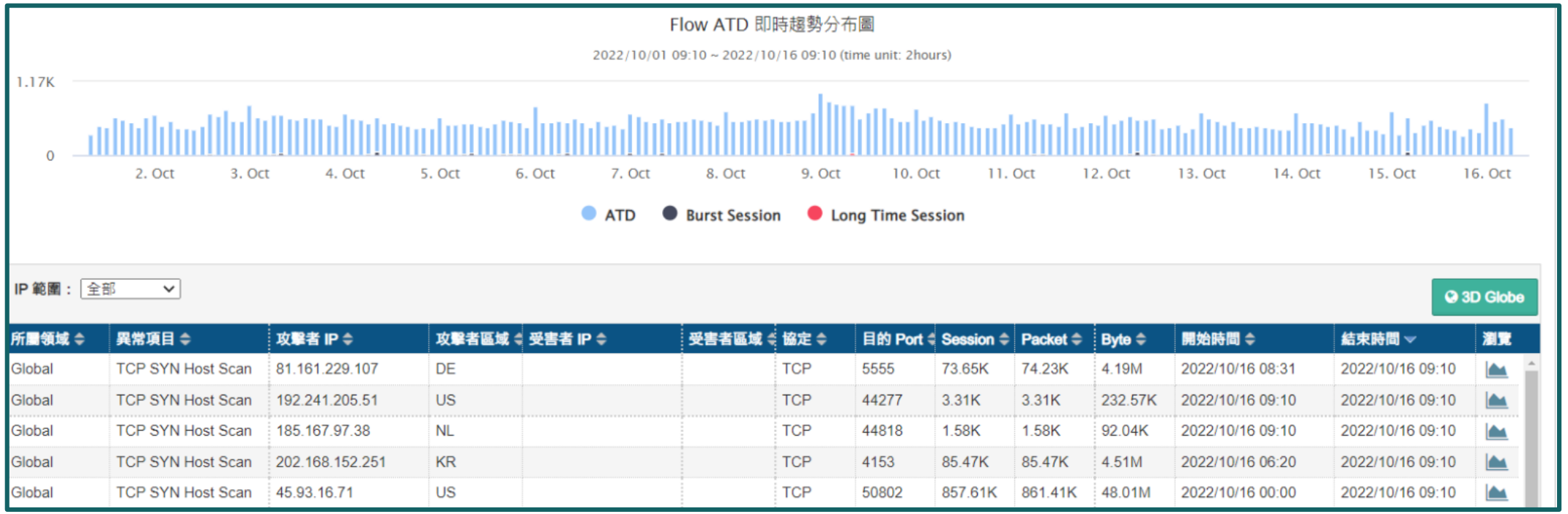
- 雙週寄發區網連線單位內的連線國家排名統計表給單位網管老師。



網路流量紀錄分析

系統網段流量異常查詢

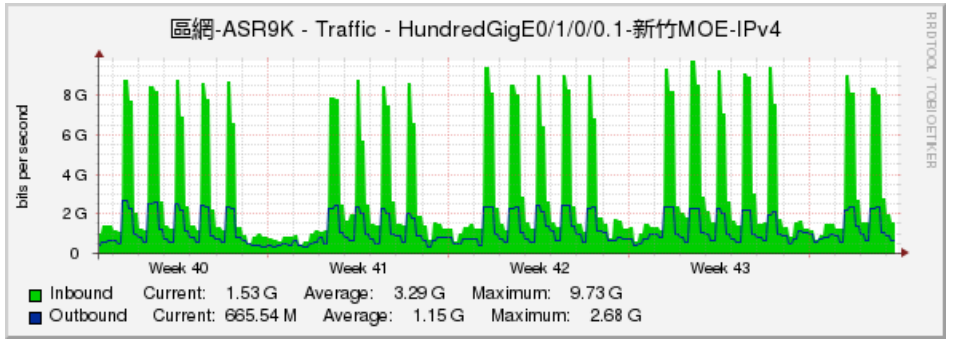
- 對DDoS、Host Scan、Port Scan等異常流量網路行為，提供各連線單位即時查詢功能。

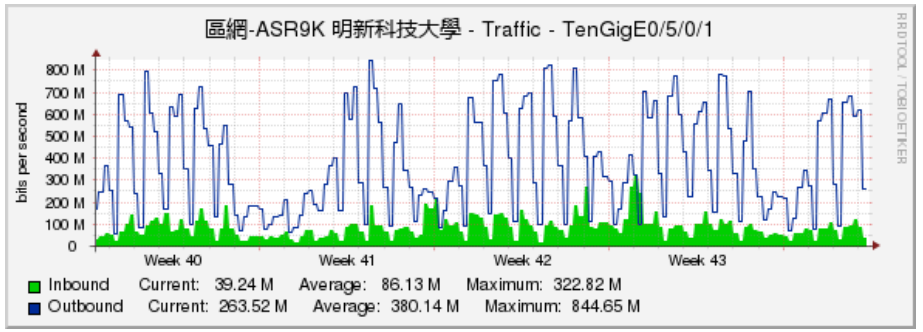


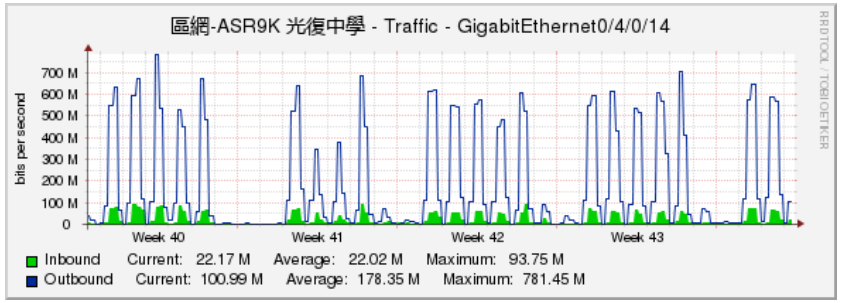
所屬領域	異常項目	攻擊者 IP	攻擊者區域	受害者 IP	受害者區域	協定	目的 Port	Session	Packet	Byte	開始時間	結束時間	瀏覽
Global	TCP SYN Host Scan	81.161.229.107	DE			TCP	5555	73.65K	74.23K	4.19M	2022/10/16 08:31	2022/10/16 09:10	
Global	TCP SYN Host Scan	192.241.205.51	US			TCP	44277	3.31K	3.31K	232.57K	2022/10/16 09:10	2022/10/16 09:10	
Global	TCP SYN Host Scan	185.167.97.38	NL			TCP	44818	1.58K	1.58K	92.04K	2022/10/16 09:10	2022/10/16 09:10	
Global	TCP SYN Host Scan	202.168.152.251	KR			TCP	4153	85.47K	85.47K	4.51M	2022/10/16 06:20	2022/10/16 09:10	
Global	TCP SYN Host Scan	45.93.16.71	US			TCP	50802	857.61K	861.41K	48.01M	2022/10/16 00:00	2022/10/16 09:10	

流量監控系統 – CACTI

- **提供歷史流量紀錄查詢**
  - 提供各連線單位流量歷史紀錄檢視：
    https://www.hcrc.edu.tw/cacti/

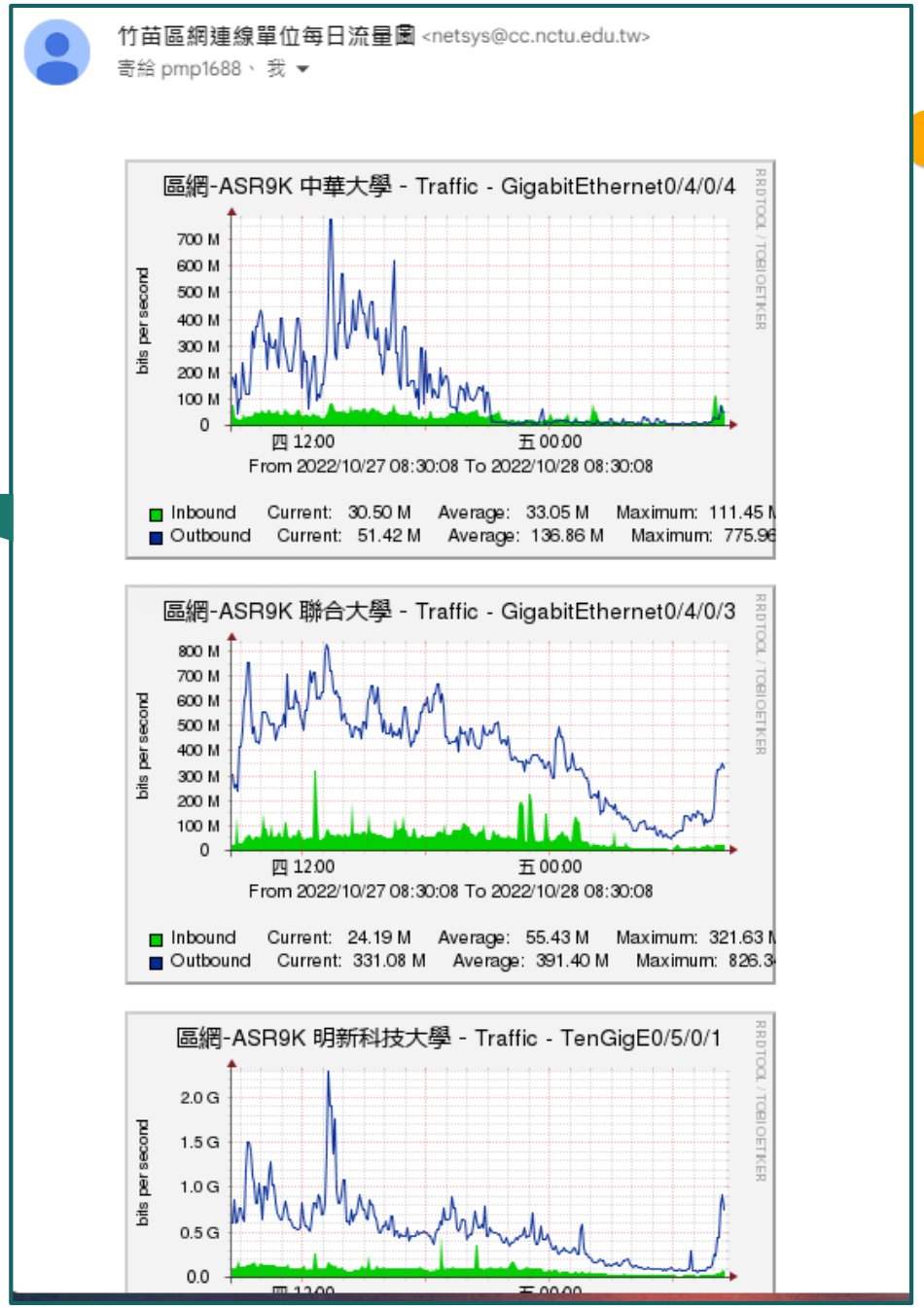






流量監控系統 — CACTI

- **每日定時寄發監控結果**
  - 各單位獨立設定網路流量圖，於每日上午8:30自動寄信通知單位網管老師前一日網路使用情形。



流量監控系統 – CACTI

- **流量承載告警通知**
  - 監控各連線單位頻寬，若頻寬承載達 **90%**，將自動寄發E-mail提醒單位網管人員。

NORMAL: 區網-ASR9K - 光復中學 - GigabitEthernet0/4/0/14 [traffic_out] [traffic_out] Restored to Normal Threshold with Value 677.5865

外部 收件匣 × HCRC × HCRC-Alarm ×

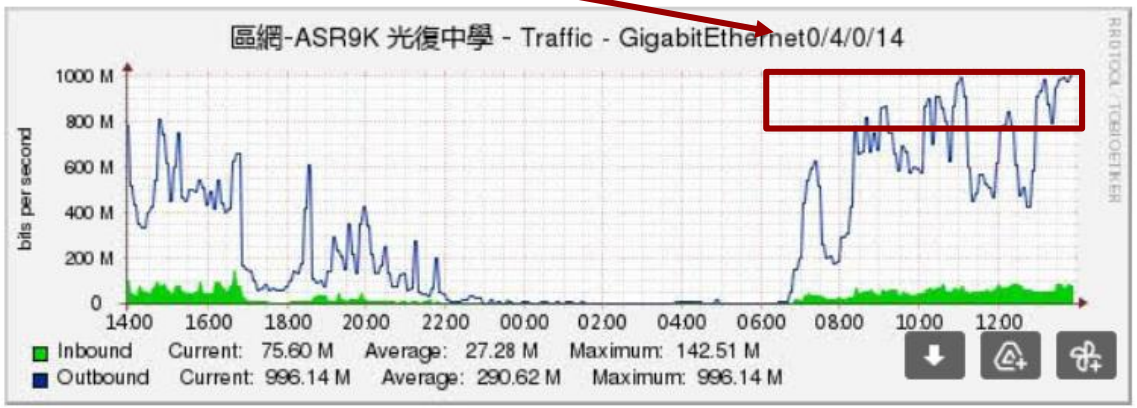
竹苗區網通知-64-160 <netsys@cc.nctu.edu.tw> 11月4日 週五 下午1:55 (3 天前)

寄給 我

英文 中文（繁體） 翻譯郵件

A warning has been issued that requires your attention.

Host: 區網-ASR9K (192.192.60.113)
URL: http://163.28.64.84/cacti//graph.php?local_graph_id=211&rra_id=1
Message: NORMAL: 區網-ASR9K - 光復中學 - GigabitEthernet0/4/0/14 [traffic_out] [traffic_out] Restored to Normal Threshold with Value 677.5865



TANET HCRC

專屬互動交流群組 – LINE

- **專屬互動分享交流群組**
  - 建立區網Line群組，能透過群組向連線單位即時提供資訊，並能讓區網夥伴快速反應問題。

漏洞資訊分享

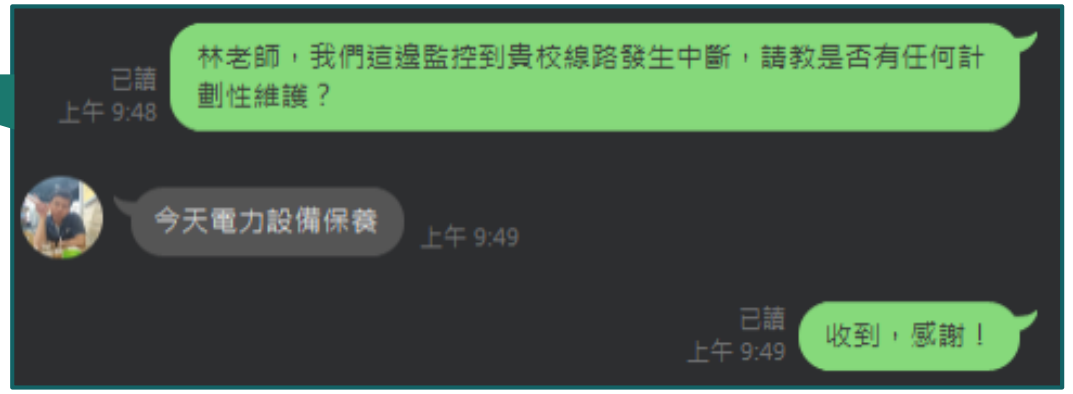
問題交流及討論

線路狀態異常即時通知 – LINE Bot

- **即時寄發通知網管人員**
  - 區網中心透過PRTG監控設備(ASR9K)上各校線路狀態，如出現異常則以LINE Notify即時通知網管人員。

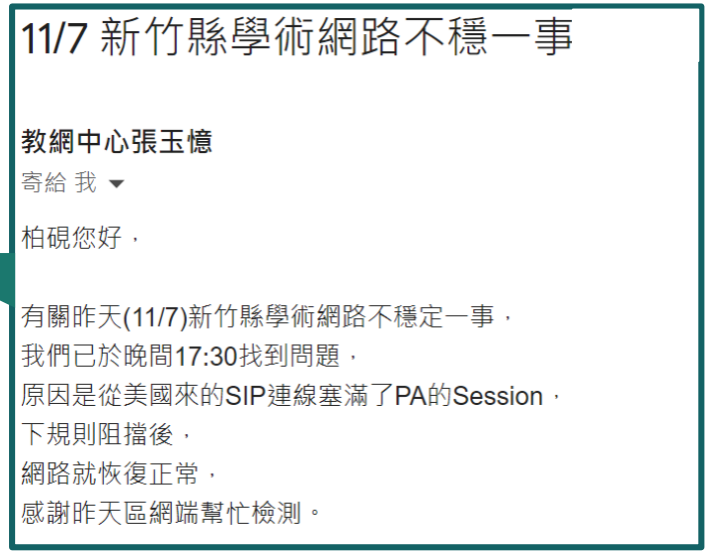
LINE Notify

- **協助進一步確認問題**
  - 由區網中心網管人員確認設備及線路狀態，並通知連線單位網管人員。



網路技術諮詢服務

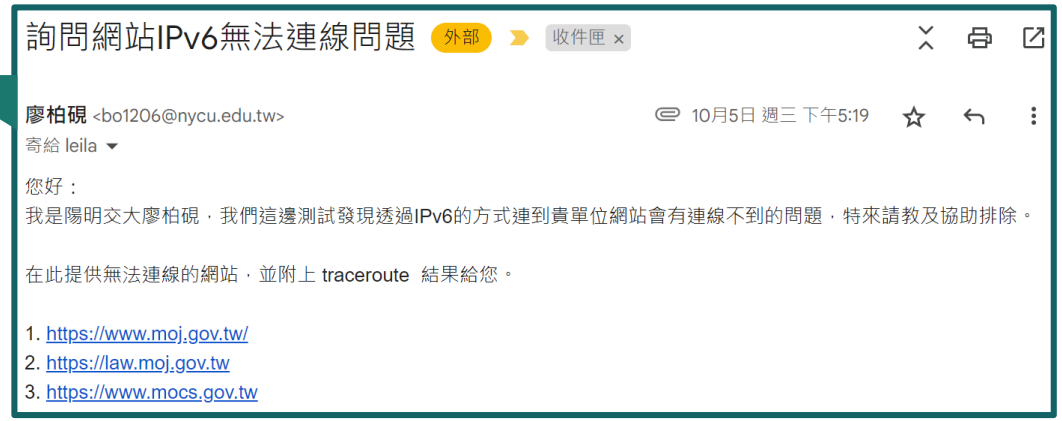
- **協助連線單位釐清並排除網路異常**
  - **案例一：單位防火牆運作異常，導致網路服務不穩定該如何處理？**
    - 處理：協助單位檢查防火牆功能，發現大量SIP連線導致防火牆異常，清除後即恢復正常服務。
  - **案例二：單位以IPv6連線至GOV網站，無法正常連線該如何排除？**
    - 處理：協助單位進行測試，並與GOV網站管理單位進行確認，發現該GOV網站路由異常，經檢修後即恢復正常。


11/7 新竹縣學術網路不穩一事

教網中心張玉憶
寄給 我

柏硯您好，

有關昨天(11/7)新竹縣學術網路不穩定一事，
我們已於晚間17:30找到問題，
原因是從美國來的SIP連線塞滿了PA的Session，
下規則阻擋後，
網路就恢復正常，
感謝昨天區網端幫忙檢測。


詢問網站IPv6無法連線問題 外部 收件匣 ×

廖柏硯 <bo1206@nycu.edu.tw> 10月5日 週三 下午5:19
寄給 leila

您好：
我是陽明交大廖柏硯，我們這邊測試發現透過IPv6的方式連到貴單位網站會有連線不到的問題，特來請教及協助排除。

在此提供無法連線的網站，並附上 traceroute 結果給您。

1. https://www.moj.gov.tw/
2. https://law.moj.gov.tw
3. https://www.mocs.gov.tw

5. 資通安全管理與應用

導入資通系統安全管理ISMS標準

- **完成竹苗區網中心111年ISO27001驗證**
  - 竹苗區網中心於101年已導入ISO 27001，並通過驗證。
  - 導入範圍包含資訊機房環境之執行、維護與管理作業流程。
  - 本年度已於111年7月完成第二年追查驗證。
  - 本中心規劃於112年度8月導入ISO27001:2022版本。

SGS

Certificate TW12/11622

The management system of

National Yang Ming Chiao Tung University

No. 1001, Daxue Rd. East Dist.,
Hsinchu City 30010, Taiwan (R.O.C.)

has been assessed and certified as meeting the requirements of

ISO/IEC 27001: 2013

For the following activities

The scope of registration appears on page 2 of this certificate.

This certificate is valid from 16 November 2021 until 18 June 2024 and remains valid subject to satisfactory surveillance audits.
Recertification audit due a minimum of 60 days before the expiration date.
Issue 7. Certified since 18 June 2012

The audit leading to this certificate commenced on 07 October 2021
Previous issue certificate validity date was until 18 June 2021

This is a multi-site certification.
Additional site details are listed on the subsequent page.

Authorised by

SGS United Kingdom Ltd
Rosemore Business Park Ellesmere Port Cheshire CH65 3EN UK
t +44 (0)151 350-6666 f +44 (0)151 350-6600 www.sgs.com

21HC 27001 2013 0421 M2

Page 1 of 2

UKAS MANAGEMENT SYSTEMS 0005

教育單位弱點檢測服務 – 網站弱掃

- **協助教育單位網站弱點檢測服務**
  - 連線單位可透過線上平台進行網站的掃描及排程掃描，並於掃描完成後將掃描結果報告以E-mail方式寄發。
  - 教育單位弱點檢測平台：https://evs.twisc.ncku.edu.tw/
  - 已掃描網站數量：21個

單位數	檢測網站數	高風險數	中風險數	低風險數	無風險數
8	21	8	3	8	3

教育單位弱點檢測服務 — 網站弱掃

- **弱點檢測服務追蹤**
  - 對於實施弱掃的單位，進行追蹤後續修補情形。
  - 針對尚未修補漏洞，皆請單位預先提出修補時程，於後續加強追蹤。

網站所屬單位	網站名稱	檢測時段	修補狀況	完成
元培醫事科技大學	yus 系統	2022-08-19 09:00:00	SSL Medium Strength Cipher Suites Supported (SWEET32), 預計2023/3/1前 升級win2019	執行中
元培醫事科技大學	系統入口網	2022-08-25 09:00:00	SSL Medium Strength Cipher Suites Supported (SWEET32), 預計2023/3/1前 升級win2019	執行中
元培醫事科技大學	APP系統	2022-08-25 01:00:00	SSL Medium Strength Cipher Suites Supported (SWEET32), 預計2023/3/1前 升級win2019	執行中
元培醫事科技大學	法規查詢系統	2022-08-25 01:00:00	Malware Identified，預計2023/3/1前改善。	執行中
元培醫事科技大學	電子公文系統	2022-08-19 17:00:00	SSL Medium Strength Cipher Suites Supported (SWEET32), 預計2023/3/1前 升級win2019	執行中
元培醫事科技大學	學校首頁	2022-08-19 09:00:00	依本校資安風險處理規定，非高風險者，無立即性威脅，暫不採取其他措施，請核閱。	完成
元培醫事科技大學	w9	2022-08-19 09:00:00	SSL Medium Strength Cipher Suites Supported (SWEET32), 預計2023/3/1前 升級win2019	執行中
元培醫事科技大學	人會總系統	2022-08-25 09:00:00	依本校資安風險處理規定，非高風險者，無立即性威脅，暫不採取其他措施，請核閱。	完成
元培醫事科技大學	校務系統學生版	2022-05-12 01:00:00	win008，OS過舊 預計2023/3/1前 升級win2019	執行中
元培醫事科技大學	校務系統職員版	2022-03-31 01:00:00	win008，OS過舊 預計2023/3/1前 升級win2019	執行中
國立新竹高中	學習歷程檔案	2020-04-20 01:00:00	轉換廠商，請廠商協助修補，並進行複掃程序	執行中
國立新竹高中	國立新竹高中校網頁	2022-06-14 00:00:00	已修補完成(目前只有6個低風險)	完成
國立竹北高中	成績處理系統	2022-05-23 01:00:00	目前已對相關廠商填寫報修單，請工程師查詢弱點並修復。	執行中
敏實科技大學	敏實科大資訊系統	2022-03-17 01:00:00	有2高風險(不含重覆風險)，1中風險。中風險因為js函式庫變更無法保證現行系統可以正常運作，預計需待學期結束後在寒假期間處理。高風險其一因網頁有字元檢查的功能故應無礙(如附件)，另一高風險因複測失敗，尚無法檢驗結果。因複測失敗於9/28再申請複測，9/30完成後，高風險剩餘1個(含重覆風險)，1中風險。中風險因為js函式庫變更無法保證現行系統可以正常運作，預計需待學期結束後在寒假期間處理。高風險因網頁有字元檢查的功能故雖有記錄但應無影響。	執行中

進度回報:【通知】貴單位於EVS平臺上有中高風險網站尚未修復-敏實科大 外部

劉得瑁 <edliu@o365.mitust.edu.tw> 2022年9月30日 上午8:32

寄給 我、evs_service@mail.moe.gov.tw、吳仁明

竹苗區網中心您好：

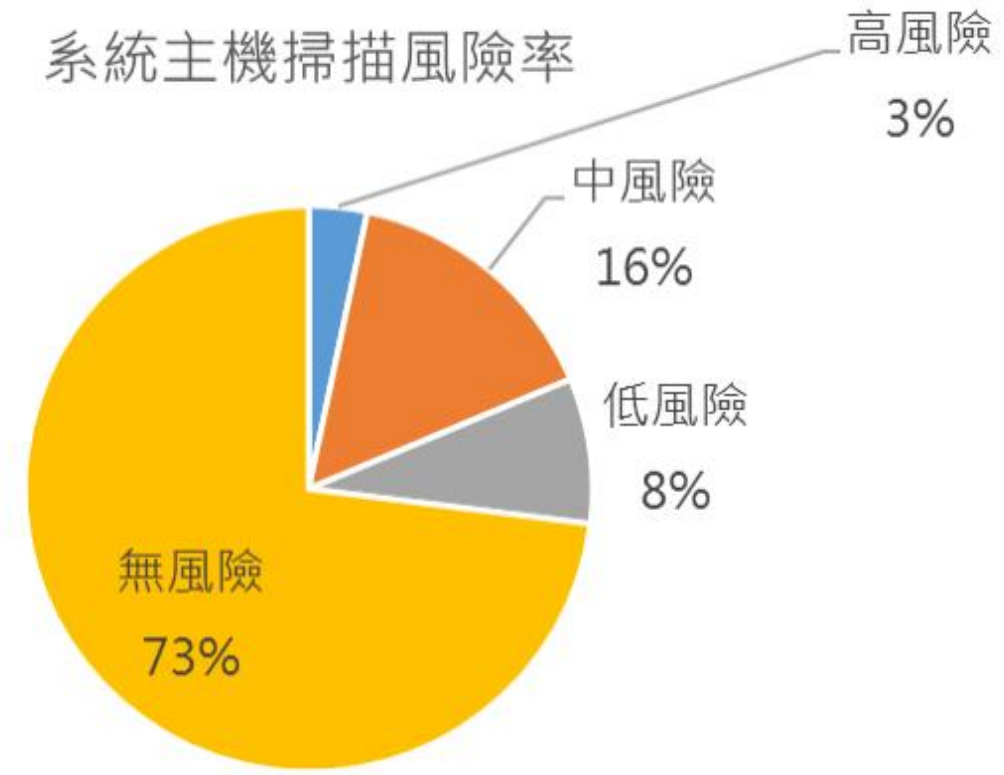
依教育部教育網站資安弱掃計畫團隊通知處理敏實科技大學EVS平臺上弱掃網站中/高風險修補，目前處理情形如下

剩餘有高風險網站ccourse.mitust.edu.tw因複測失敗於9/28再申請複測，9/30完成後，高風險剩餘1個(含重覆風險)，1中風險。中風險因為js函式庫變更無法保證現行系統可以正常運作，預計需待學期結束後在寒假期間處理。高風險因網頁有字元檢查的功能故雖有記錄但應無礙(網頁安全機制如附件)。

剩餘中/高風險待複測處理完成後再回報，謝謝。

教育單位弱點檢測服務 – 主機弱掃

- **協助連線單位系統主機弱點檢測服務**
  - 提供連線單位檢測系統主機服務(Nessus)，並追蹤後續修補狀況。
  - 已完成掃描主機數量：241台
  - 其中發現高風險約有3%，中風險約有16%



教育單位弱點檢測服務 – 主機弱掃

主機弱點檢測服務追蹤

- 對於實施主機弱掃的單位，進行追蹤後續修補情形。
- 針對尚未修補漏洞，皆聯絡請單位預先提出修補時程，於後續加強追蹤。

文件編號	ISMS-D-36-B11	文件名稱	版本	1.1
制定單位	資訊中心	弱點處理報告單	機密等級	限閱

紀錄編號：_____ 填表日期：111年8月3日

設備/系統名稱		設備/系統負責人		檢測日期： 111 年 07 月 01 日
設備/系統網址：		內/外部 IP		應回覆時間： 年 月 日

編號	弱點名稱	等級	修補作業說明	修補日期	無法修補原因與防禦因應方法
1	Cross Site Scripting (Reflected)	High	增加 NGINX 設定，封鎖所有跨站請求	111/8/3	
2	Content Security Policy (CSP) Header Not Set	Medium	增加 NGINX 設定，封鎖所有跨站請求	111/8/3	
3	Missing Anti-clickjacking Header	Medium	增加 NGINX 設定，封鎖所有跨站請求	111/8/3	
4	Vulnerable JS Library	Medium	更新 jquery ui 為當前最新版本(1.13.2)	111/8/3	
5	TLS Version 1.1 Protocol Deprecated	Medium	停用 TLS Version 1.1	111/8/3	
設備負責人核章			權責主管核章		

【網站弱掃】有關https:/ .nycu.edu.tw/網站之弱點掃描報告結果 垃圾桶 ×

寄給 nycu.edu.tw nycu.edu.tw、 @nycu.edu.tw、 7月28日 週四 上午9:49

老師您好

此為貴單位網站之初次弱點掃描報告(如附件)，內含：

1. 網站弱點掃描報告html檔。
2. 主機弱點掃描報告html檔，若為本校Cpanel服務則主機弱點由本中心服務負責人進行修補作業。

※檔案因具機敏性，故加密，加密密碼(共10碼)為：**本校校名英文縮寫大寫四碼@您的分機。**

1. 修補作業：
1. **高中風險弱點修補，除有技術面合理說明或其他因應策略，並經單位主管確認者外，均應進行修補。**
2. 高風險弱點未完成修補期間，應每日自行檢查及確認網站運作狀況，並留存檢查及修補記錄 。
3. 針對高風險弱點，各業務負責人應確實填寫**弱點處理報告單(請至公告內下載https://it.nycu.edu.tw/news/8307/)**，並由各單位主管進行確認後，於**8/29(一)前簽核掃描回覆郵件**。
4. 單位網站若有維護廠商或人員，可提供弱點掃描報告請其修補填寫弱點處理報告單內容後，由網站負責人確認簽核。
5. 本次檢測之各項網站弱點，將於下次進行弱點掃描時再次進行追蹤與確認。
6. **若無高中風險之單位網址，則無需回傳弱點處理報告單。**

謝謝您！

若有相關問題，則可聯繫以下人員：
資訊技術服務中心 網路系統組

資安事件通報統計

資料統計：2022/1/1-2022/9/30

1、2級資安事件處理	
● 通報平均時數	0.07 Hrs
● 應變處理平均時數	0.58 Hrs
● 事件處理平均時數	1.27 Hrs
● 通報完成率	99.25%
● 事件完成率	97.01%
3、4級資安事件通報	無
資安事件通報審核	
審核平均時數	0.66 Hrs
聯絡相關資訊完整度	94.12%

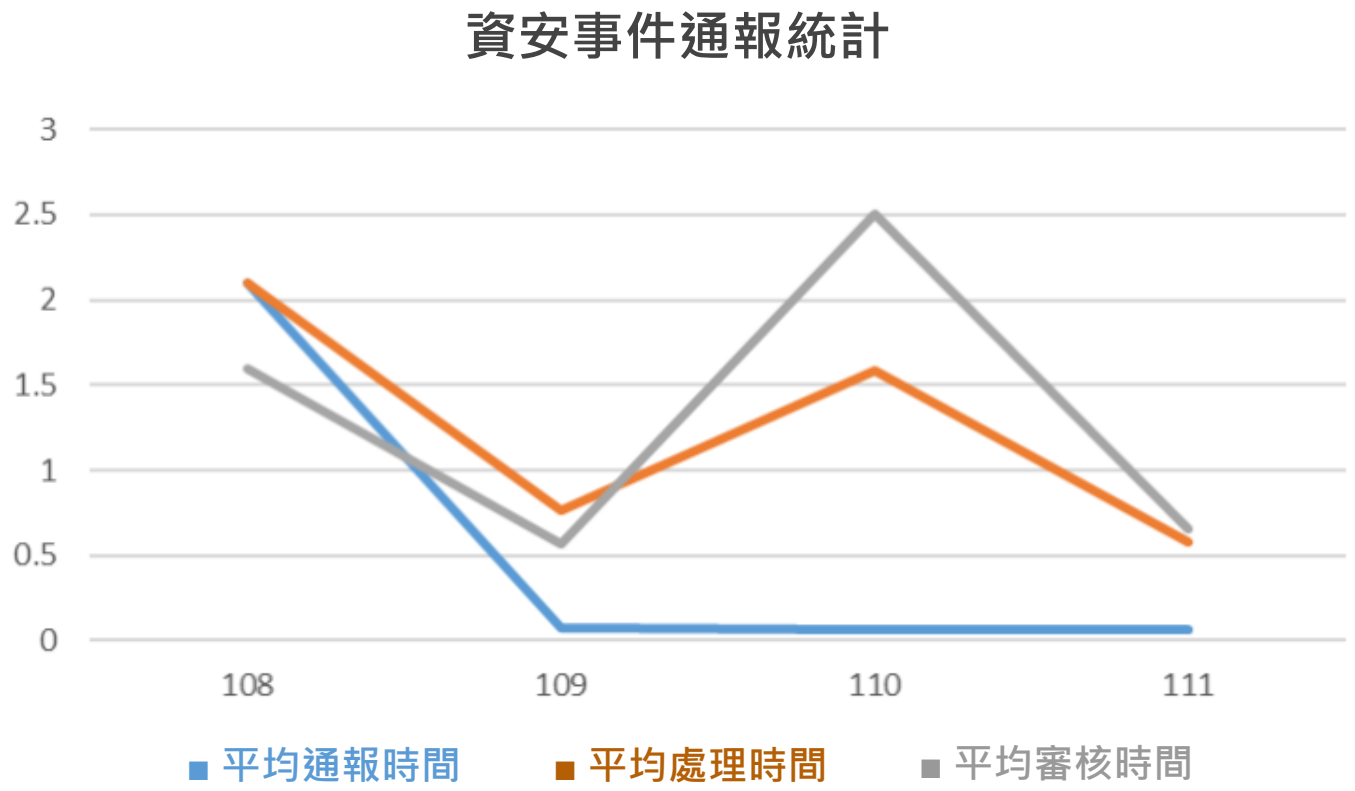
- 由於疫情期間居家辦公因素，單位在事件處理上較無法即時完成，導致通報及事件完成率較低。
- 後續已強化與單位通報作業處理，如第二、三聯絡人。

- 世界高中於整備期間發生人員離職，未能順利完成交接程序，導致未能修改聯絡資料。
- 已修正聯絡資訊，並於後續強化宣導人員變更管理。

歷年資安事件通報統計

加速通報處理速率

- 今年度資安事件通報平均審核時間，相較去年加速了約1.84個小時；平均處理時間整體加速約 1 小時。

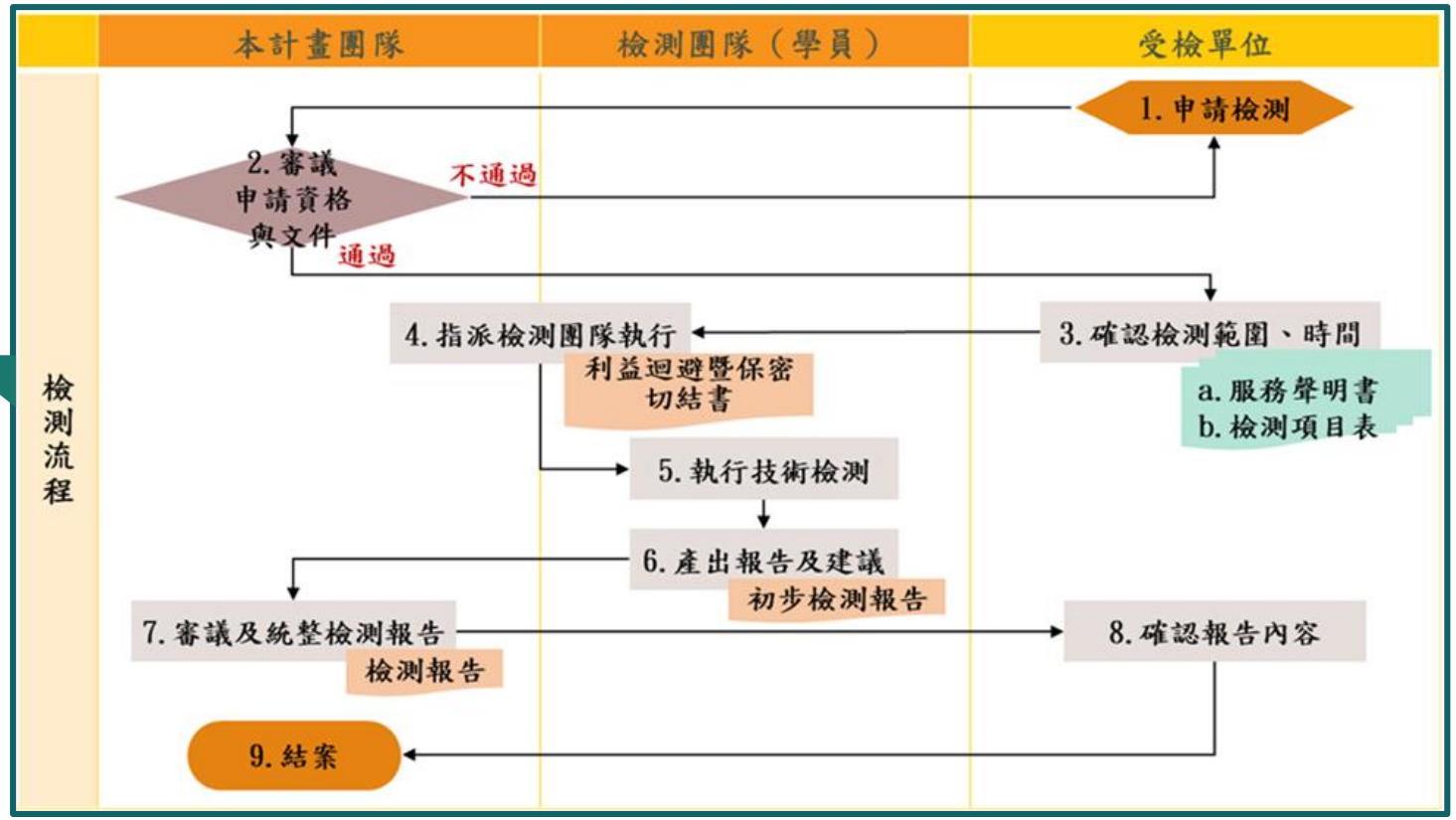


6. 應用創新服務

資通系統安全檢測服務

協助單位發掘潛在風險

- 本中心提供連線單位「資通系統安全檢測」服務申請，安排通過資安專業認證之竹苗地區資安相關系所學生實施內網滲透測試。



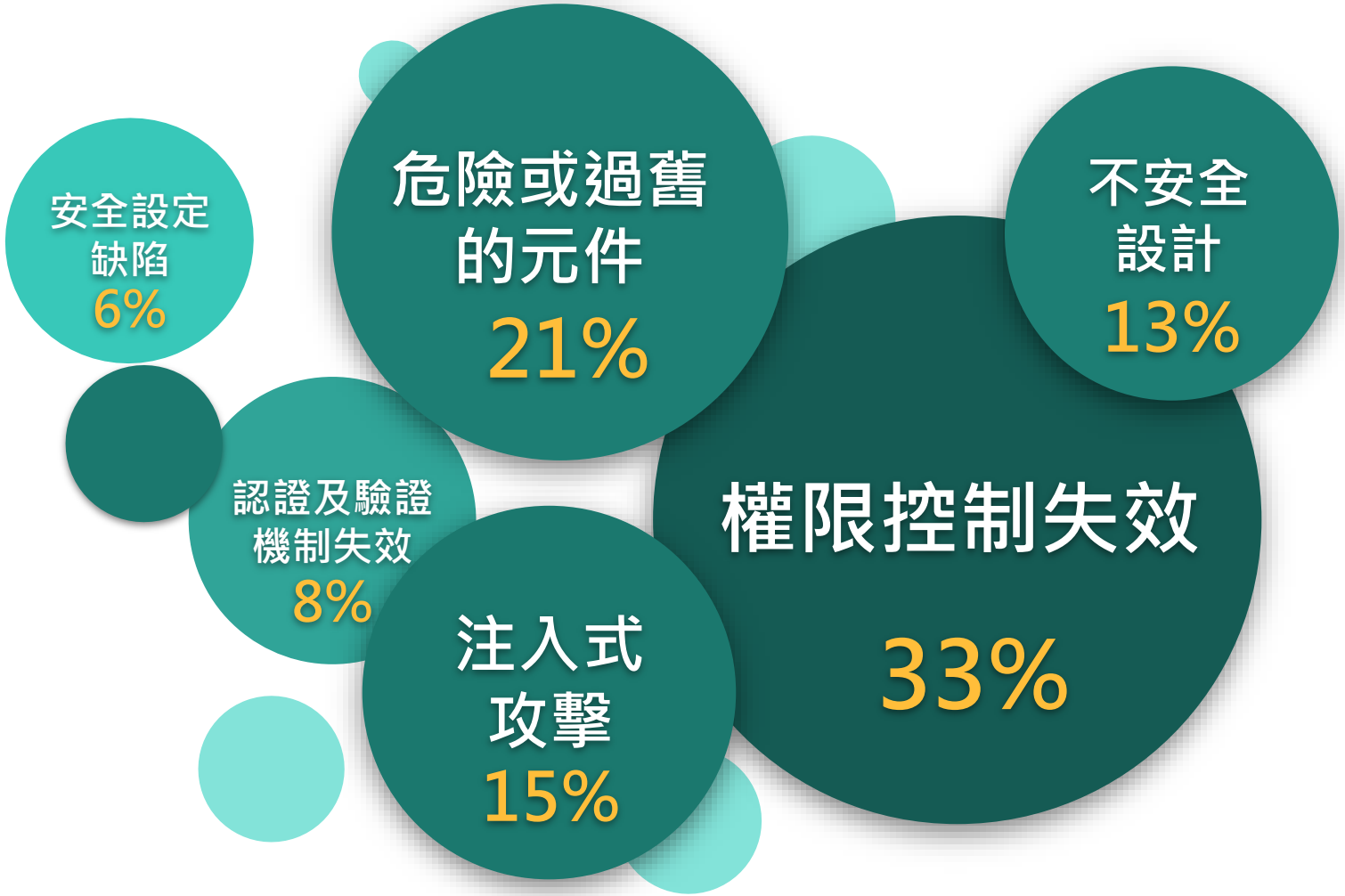
TANet HCRC

資通系統安全檢測服務成果

- 本年度完成 **5** 案區網連線單位資通系統安全檢測服務。
- 累計完成 **21** 個系統，共發掘 **103** 個潛在風險。
- 其中高風險約佔 **20%**，中風險約佔 **40%**。

國立新竹高級中學	新竹縣教育網路中心	國立陽明交通大學	育達科技大學	國立新竹科學園區實驗高級中等學校
				
111年8月9-10日	111年8月23-24日	111年９月1-2日	111年11月15-16日(遠端)	111年11月15-16日(遠端)

資通系統安全檢測服務結果統計

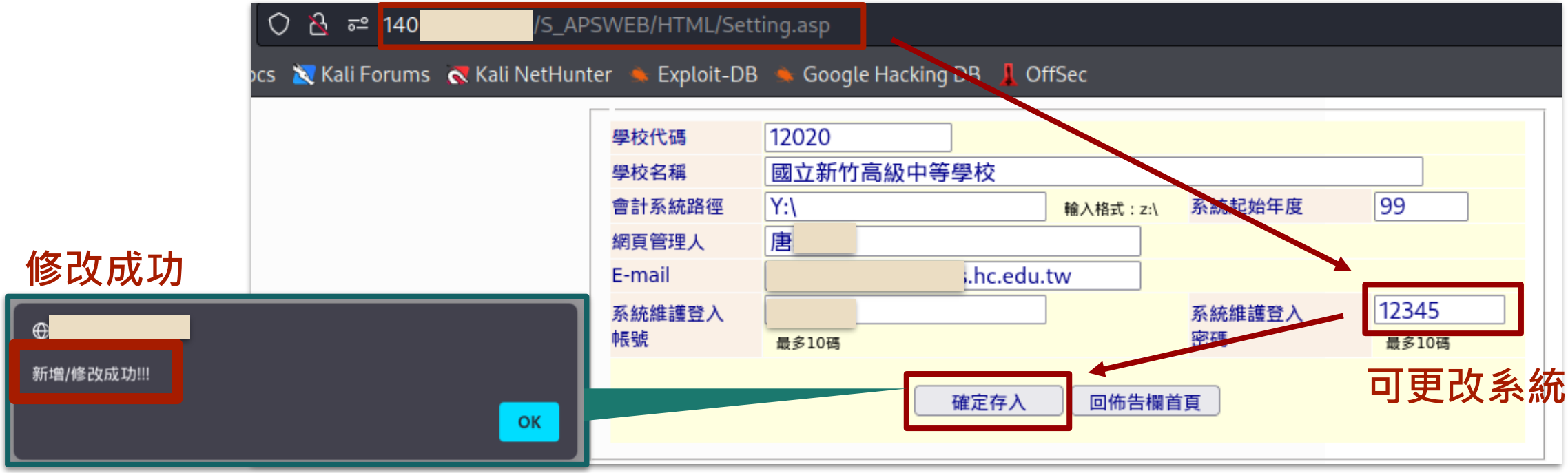


TANet HCRC

資通系統安全檢測服務案例 – 國立新竹高中

- 全國國立高中使用之「國立高級中等學校校務基金網路請購系統」
  - 取得管理者設定路徑，**無須其他權限即可修改管理者資訊－高風險**。
    - 全國國立高中皆使用該套系統，發現漏洞後即提供教育部進行修補參考。

國立社教機構作業基金及國立高級中等學校校務基金網路請購系統



資通系統安全檢測服務案例 — 新竹縣教網中心

- 新竹縣教育研究發展暨網路中心之「校務行政系統」
  - 主機應用系統pkexec存在CVE-2021-4034 (CVSS 7.8)，可使一般使用者直接提權至最高管理者(root)－高風險。

```
nycutest1@sch137:~$ ip a show dev ens160
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:92:89:33 brd ff:ff:ff:ff:ff:ff
    inet [redacted]/24 brd [redacted] scope global ens160
       valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:fe92:8933/64 scope link
       valid_lft forever preferred_lft forever
nycutest1@sch137:~$ id
uid=1005(nycutest1) gid=1002(nycutest1) groups=1002(nycutest1)
nycutest1@sch137:~$ /tmp/PwnKit
root@sch137:/home/nycutest1# id
uid=0(root) gid=0(root) groups=0(root),1002(nycutest1)
```

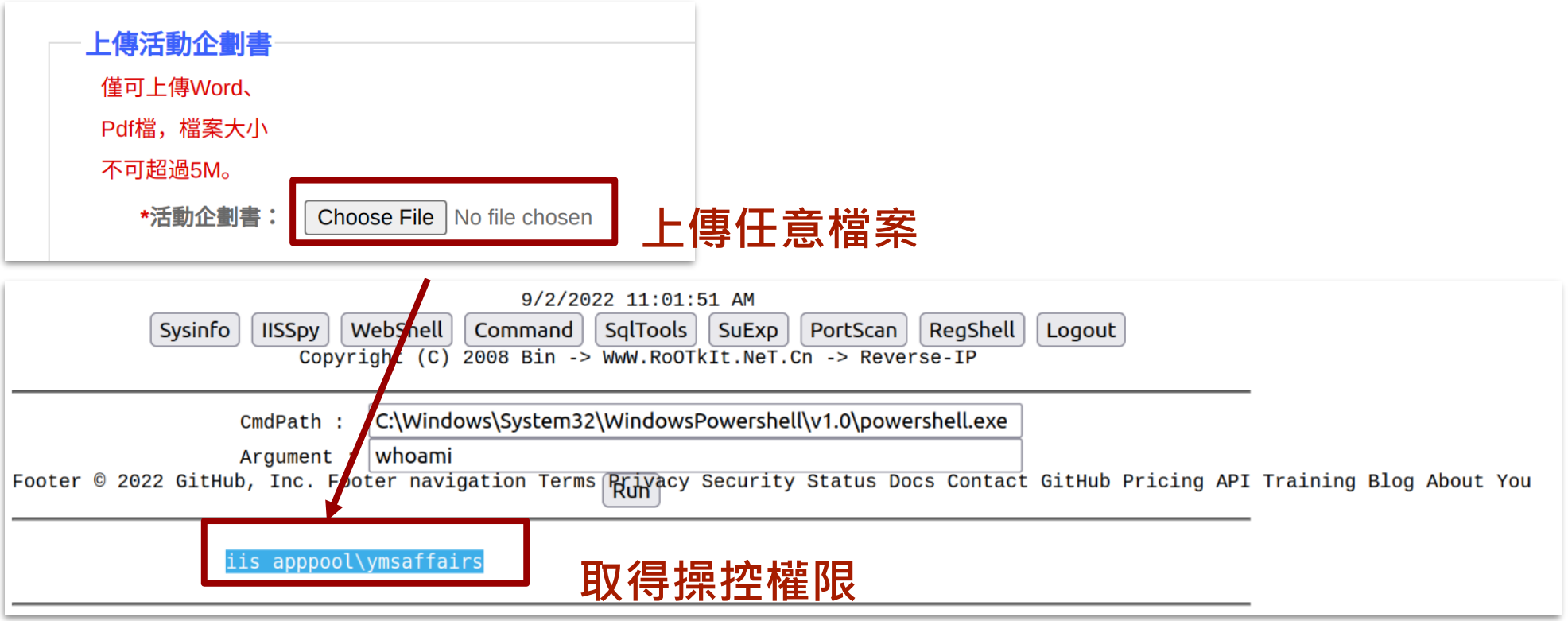
原一般使用者

成功變更為最高管理者

TANet HCRC

資通系統安全檢測服務案例 – 國立陽明交通大學

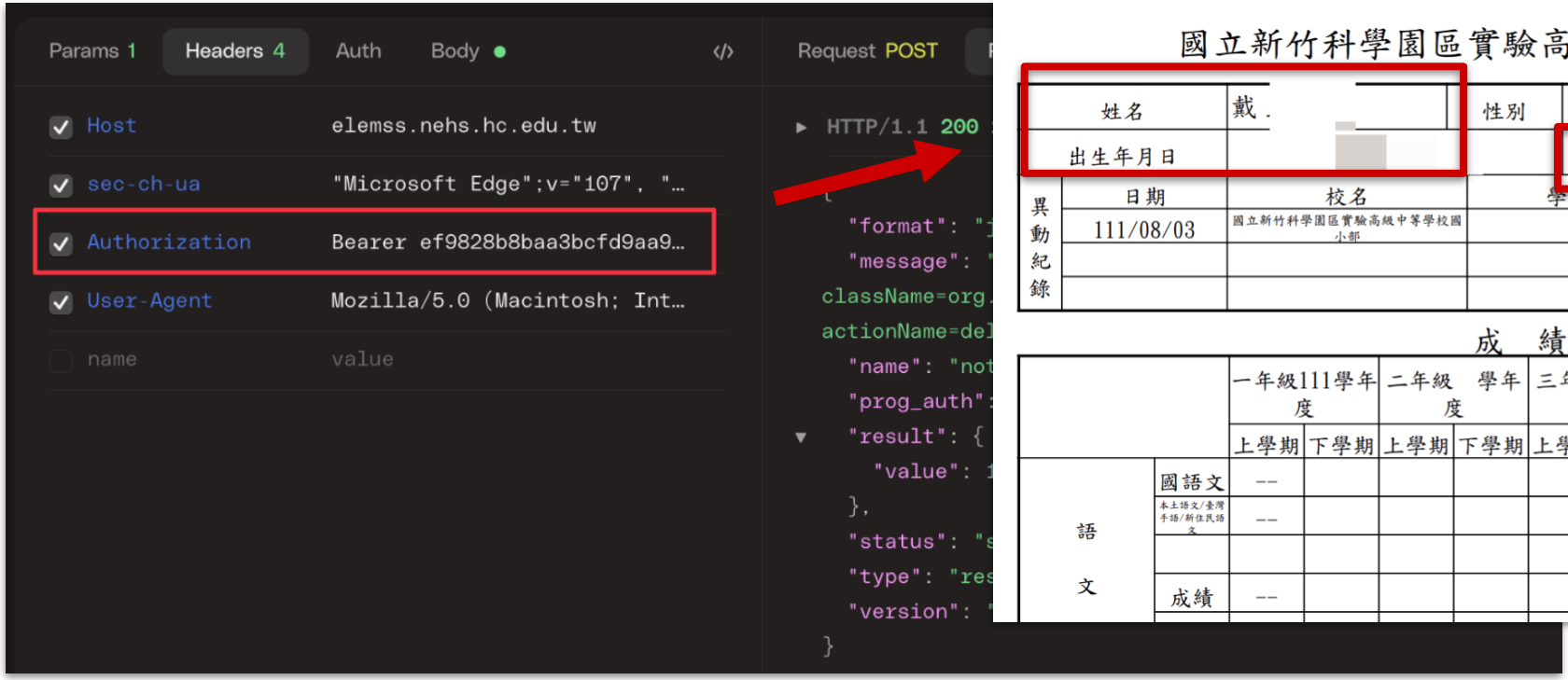
- 國立陽明交通大學之「學務資訊系統」
  - 一般使用者可上傳其他網頁檔案，**無須授權可取得操控權限(Web shell)**
    – **高風險**。

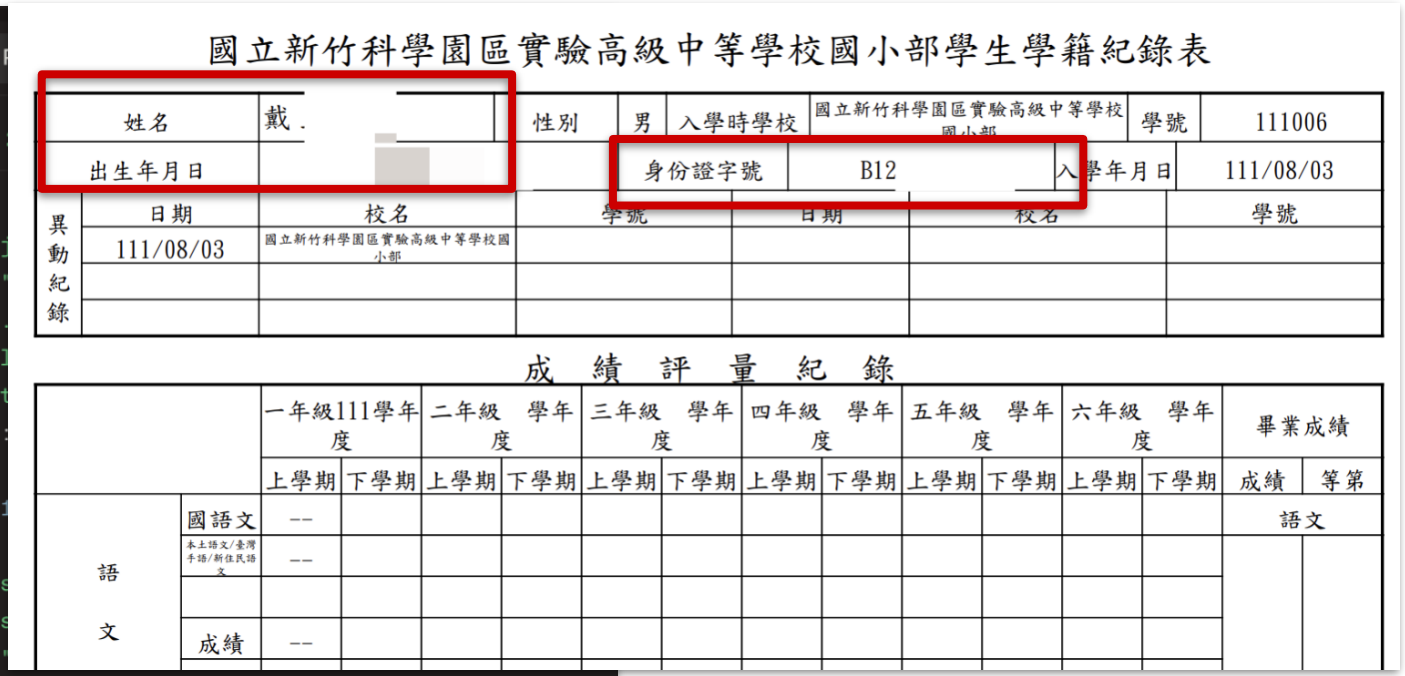


TANet HCRC

資通系統安全檢測服務案例 – 國立新竹園區實驗中學

- **國立新竹園區實驗高級中等學校之「國小部教訓輔系統」**
  - 科任老師的存取認證碼(Access Token)可獲得教務組長權限，透過列印學籍資料卡，**可獲得全校學生身份證字號/生日/姓名－高風險**。





國立新竹科學園區實驗高級中等學校國小部學生學籍紀錄表

姓名	戴	性別	男	入學時學校	國立新竹科學園區實驗高級中等學校國小部	學號	111006
出生年月日				身份證字號	B12	入學年月日	111/08/03

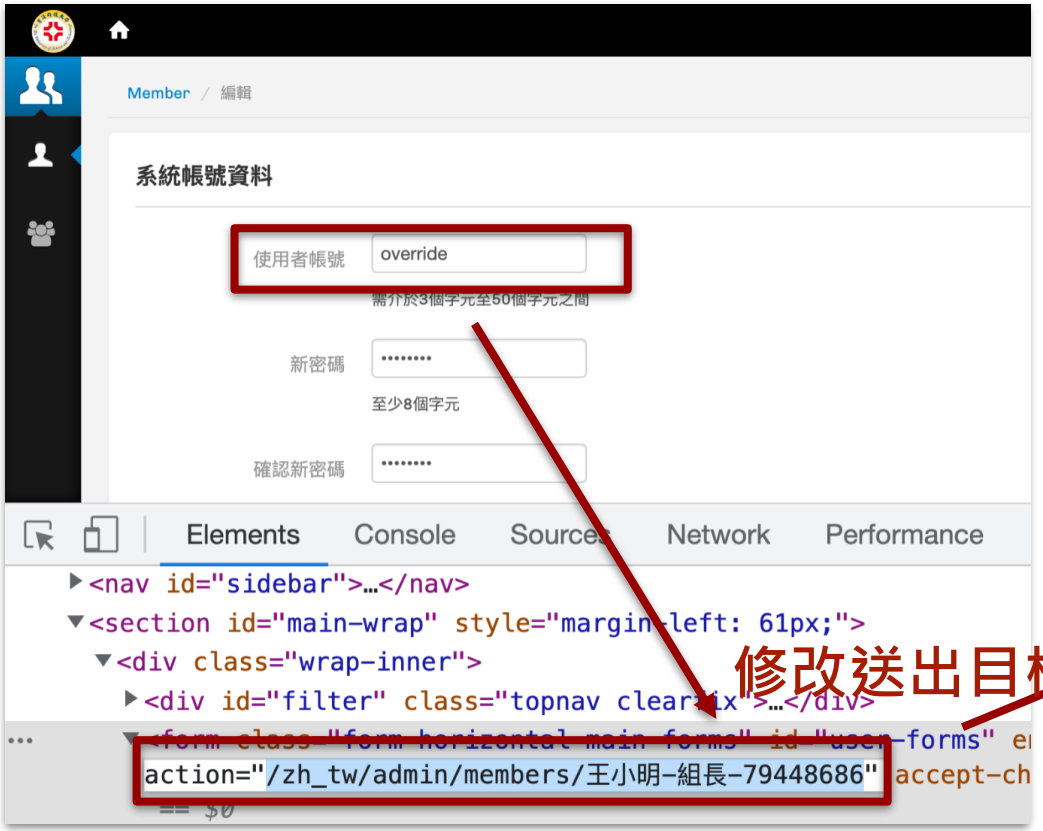
異動紀錄	日期	校名	學號	日期	校名	學號
	111/08/03	國立新竹科學園區實驗高級中等學校國小部				

成績評量紀錄

		一年級111學年度		二年級 學年度		三年級 學年度		四年級 學年度		五年級 學年度		六年級 學年度		畢業成績	
		上學期	下學期	上學期	下學期	上學期	下學期	上學期	下學期	上學期	下學期	上學期	下學期	成績	等第
語文	國語文	--												語文	
	本土語文/臺灣手語/新住民語文	--													
	成績	--													

資通系統安全檢測服務案例 – 育達科技大學

- 育達科技大學之「招生資訊網」
  - 帳號編輯頁面修改送出目標，可修改目標使用者任意資料(包含密碼) – 高風險



修改送出目標

TANET論文投稿

- TANET論文研討
  - 今年(111)度於TANET論文研討會進行投稿，本次共 2 篇入選。

教育體系資安技術檢測作業實務研究與探討

何馨晴
國立陽明交通大學
資訊技術服務中心
heather.sc@nycu.edu.tw

林鉦烜
教育部
資訊及科技教育司
esora@mail.moe.gov.tw

高義智
國立陽明交通大學
資訊技術服務中心
ykao@nycu.edu.tw

摘要

現今資通訊技術迅速發展，在這資安事件極為頻繁的時代，尚有教育體系單位受歷史包袱使用老舊資通系統，或未發覺正採用具高風險設備及環境架構，這些資通訊設備維護更新皆需知能及資源，但多數單位處於技術人才不敷需求、經費受限的問題，面臨資源匱乏與資安風險議題的窘境，更是缺少推動近年《資通安全管理法》[1]上路的檢測作業能量。本研究獲教育部贊助與支持推動教育體系資安檢測技術服務作業，協助教育部檢視教育體系資安法遵技術面落實情形，藉此發現單位潛在資安風險，並提供改善建議，迄今已完成30多案教育體系資安技術檢測作業，發掘上千筆潛在漏洞，其中高風險問題約10%、中風險約30%，亦協助追蹤歷案檢測缺失改善情形，排除數百件資安問題，更依歷次作業經驗彙整常見資安缺失及安全漏洞，提供教育體系各單位相關建議及推廣防護知識，期逐步提升教育體系資通安全環境。

關鍵詞：滲透測試、弱點掃描、資安健診

Abstract

Information and communication technology is developing rapidly nowadays. In this era of extremely frequent information security incidents, there are still educational units burdened by history using outdated systems, or not aware of the use of high-risk equipment and system technology testing operations in the education system. It has been found thousands of potential vulnerabilities, of which about 10% are high-risk problems and about 30% are medium-risk problems. They also help track the lack of improvement in the detection of historical cases, and eliminate hundreds of information security problems. It also compiles common information security deficiencies and security vulnerabilities based on previous operating experience, provides relevant suggestions for each unit of the education system and promotes protection knowledge, and hopes to gradually improve the information security environment of the education system.

Keywords: penetration testing, vulnerability scanning, information security health diagnosis

1. 前言

1.1 研究動機

隨著《資通安全管理法》於108年的正式實施，教育體系單位對於該如何落實應辦事項繁多的資安法遵陷入了窘境，以及面對現今資訊發展快速，資安威脅層出不窮，技術資源及管理觀念無法即時負荷的教育單位即成為惡意人士利用的練習標的，此時更明顯點出單位即時更新修補及長期防護維運能量的不足，進而延伸教育體系欠缺資安推動人力的議題。以下本研究動機將分為兩點說明：

7. 111年度計畫績效指標辦理情形

年度績效指標辦理情形

- 本年度績效指標完成率皆為 **100%**，全數達標。

類型	項目	進度	完成率
ISMS驗證	於111年7月前重新驗證ISMS	本年度於111年7月20日完成重新驗證	100%
骨幹網路服務	竹苗區網中心對TANet骨幹網路服務可用率達99.5%	111年度竹苗區網中心對TANet骨幹網路服務可用率達99.99%	100%
技術教育訓練	協助連線學校教職員參與資安或網路技術教育訓練至少200人次	111年度總共辦理6場教育訓練課程，參與人員達243人次。	100%
資安服務	協助至少5所連線學校進行網站弱點掃描、健檢等資安服務	已完成執行8所單位，共21個網站弱點掃描，並且協助12間單位共223台主機弱點掃描。	100%
無線網路漫遊服務	協助至少3所連線單位導入eduroam無線網路漫遊服務	光復高中、曙光女中、苗栗縣網中心	100%

111年度服務滿意度調查

- 本年度貴校(單位)如有網路管理或連線的技術諮詢時，區網中心的協助是否符合您的需求？
- 貴校(單位)對於區網中心服務人員之熱忱及親和力的滿意度？
- 對區網所舉辦之教育訓練或研討(習)課程，是否能符合貴校(單位)實務運作上的需求？
- 本年度區網中心對貴校(單位)之網路連線服務，您認為是否順暢？

發現多為中華電信線路查修時造成意外斷線。

- 本年度貴校(單位)如有資通安全事件的通報應變需協助處理時，區網中心的協助是否符合您的需求？

因單位人員於疫情期間居家辦公造成部分聯繫較無法完全即時。

- 本年度區網中心對貴校(單位)聯繫協調與溝通管道上，您認為是否順暢？

8. 112年度預計推動之重點工作

112年度預計推動之重點工作

1. 【機房維運】：持續維護管理機房設備及環境，提供更良好網路運作。
2. 【網路可用率】：持續維護及監控網路狀態，提供最即時的網路資訊，目標網路可用率達99.95%以上。
3. 【服務建置】：持續推動及建置各連線單位IPv6 Web及DNS服務。
4. 【教育訓練】：規劃場辦理7場資安及網路管理相關教育訓練課程，以提升連線單位網管人員資通訊安全能力。
5. 【管理委員會議】：辦理2場區域網路管理委員會，以加深連線單位之間的交流。

112年度預計推動之重點工作

6. 【ISO驗證】：持續導入ISO27001，並重新驗證ISO27001。
7. 【資安通報】：持續精進配合教育部資通安全通報相關事項，加強協助連線單位處理通報事項，以提高各單位回報時間，加強單位聯絡資訊更新，使完整度達100%。
8. 【流量分析】：持續提供連線單位Netflow異常網路封包分析服務，提供網管人員對於資安通報內容上進行查詢功能，以達到縮短網路異常檢測時間。

112年度預計推動之重點工作

9. 【弱點掃描服務】：持續提供連線單位申請主機系統弱點掃描之服務，並且追蹤協助後續修補狀況。近期已採購網站弱掃軟體(Appscan)將提供連線單位申請檢測服務。

10. 【資通系統安全檢測服務】：持續提供連線單位申請資通系統安全檢測服務，並協助追蹤後續修補狀況。

11. 【網路架構升級】：升級竹苗區網資安架構，擴充現有的Bypass交換器的模組，以達到頻寬擴充；新增一台分流器，規劃將利用新的分流器執行分流功能，而舊的分流器將執行Netflow的流量導入，藉此降低目前分流器的處理效能不足之問題。

Thanks !