



宜蘭區網中心

# 110年執行成效報告

報告人: 郭芳璋 館長

## ➤ 基礎維運

- 區網中心基本資料及人力
- 區網中心網路架構
- 網路管理維運具體辦理事項
- 資訊安全環境整備
- 資安服務維運具體辦理事項

# 區網中心基本資料及人力(1/2)

- 單位地址：26047宜蘭縣宜蘭市神農路一段一號
- 網址：<https://www.ilrc.edu.tw>
- 專任人員**2名**、兼任人員**5名**

職稱	姓名	連絡電話	TANet VoIP	電子郵件	業務職掌
主任	郭芳璋	03-9317110	94207110	kfc@niu.edu.tw	綜理區網中心業務
執行秘書	簡立仁	03-9317125	94207125	lrjen@niu.edu.tw	協助主任綜理區網中心業務
技術師	曾國旭	03-9317126	94207126	khtzeng@niu.edu.tw	資安業務與骨幹維護
技術師	游育豪	03-9317127	94207127	yuhao@niu.edu.tw	網路電話與網頁維護
技術師	施衣喬	03-9317112	94207122	golsip@niu.edu.tw	資安業務與骨幹維護
專任助理	林子為	03-9317128	94207128	zwlin@niu.edu.tw	網路電話與資安業務
專任助理	莊智傑	03-9317128	94207129	chihchieh@niu.edu.tw	網路管理、網站應用程式弱點監測平台、防洩漏個資掃描平台

## 區網中心基本資料及人力(2/2)

▶ 縣網中心 x 1，連線頻寬 4 Gbps

【連線單位數: 17】

### ● 大專院校 x 5

宜蘭大學 20Gbps

佛光大學 500Mbps

蘭陽技術學院 200Mbps

聖母專校 100Mbps

耕莘專校宜蘭校區 100Mbps

### ● 高中職 x 11

國立宜蘭高中 1 Gbps

國立蘭陽女中 300 Mbps

國立羅東高中 100 Mbps

國立頭城家商 100 Mbps

國立宜蘭高商 300 Mbps

國立宜蘭特殊教育學校 300 Mbps

國立羅東高商 300 Mbps

國立羅東高工 50 Mbps

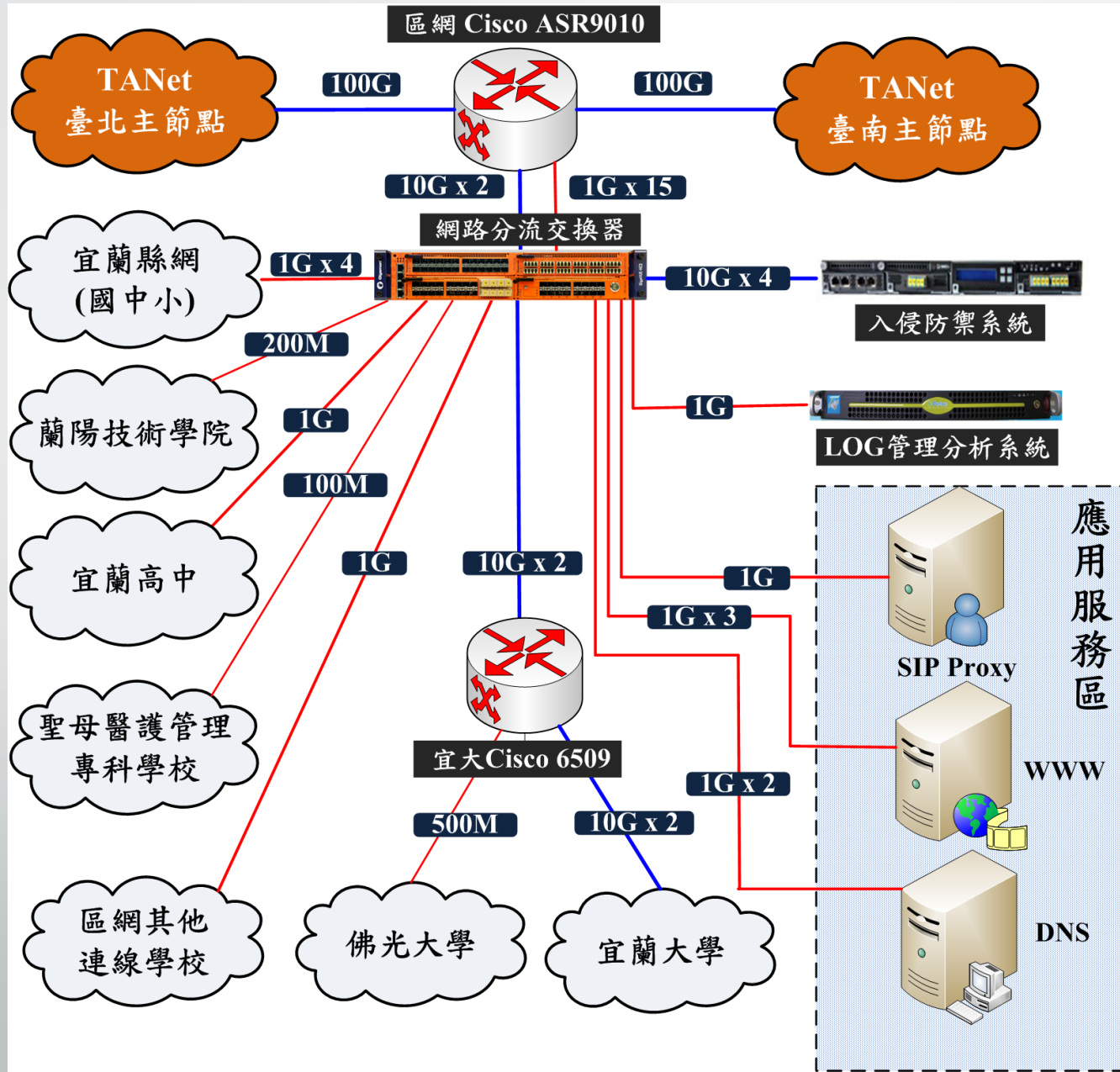
國立蘇澳海事 300 Mbps

私立中道國際中小學 50 Mbps

私立慧燈中學 50 Mbps

# 宜蘭區網中心網路架構

5



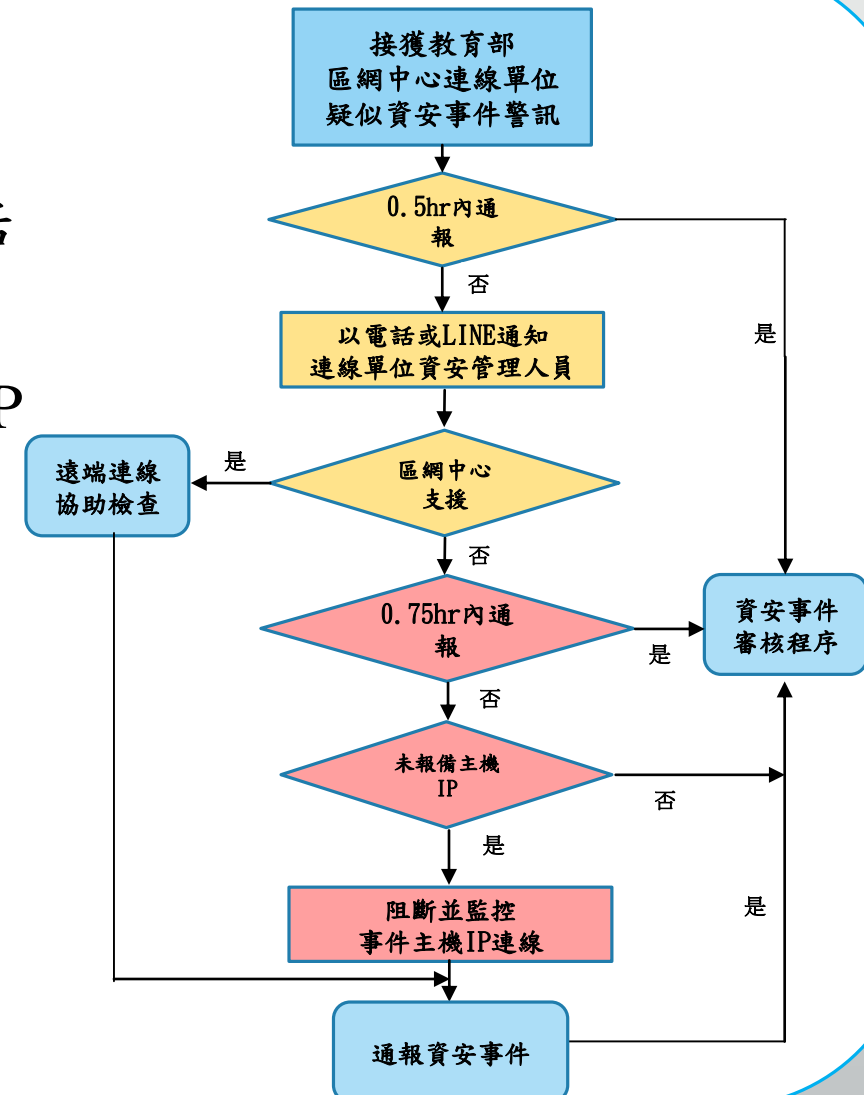
## 網路管理維運具體辦理事項

- 連線單位流量管理與連線監控：透過相關工具與系統，以了解連線單位網路使用情形。**本年度主動通知連線單位斷線共2次。**
- 網路設備管理：無任何故障紀錄。每週四透過資安人員從TACERT網頁下載TOP 500惡意IP位址，編寫成ACL後再匯入ASR9010，以阻擋惡意連線。
- 配合教育部國教署高級中等學校以下學校核心系統向上集中政策，收容DNS及WWW主機。**目前DNS主機已全部向上集中，WWW主機已收10所。**
- 連線單位網管業務諮詢及到校輔導服務。
- 區網中心網頁維護：不定時加入最新資訊，以符合現況。

# 資訊安全環境整備(1/3)

7

- 1小時內通報時程的掌握
  - 0.5hr未通報，會先以LINE或電話聯絡連線單位
  - 0.75hr未通報，擬封鎖連線單位IP
- 0.75hr未通報，封鎖連線單位IP
  - 需事先調查連線單位不能封鎖之IP
  - 當發生資安事件，未完成通報，且未事先報備之IP則暫時封鎖該IP





## 資訊安全環境整備(2/3)

### ▶ 教育機構資安通報平台

本年度於**9月6日~10日**進行**連線單位通報演練**，所有連線單位均能於**時限內完成事件通報**

本年度1、2級資安事件通報平均時數為**0.04小時**，事件處理平均時數為**0.32小時**，無3、4級資安事件。  
區網中心審核平均時數為**0.18小時**

連線單位聯絡資訊**完整度100%**



## 資訊安全環境整備(3/3)

- ▶ 資安證照(圖書資訊館人員)
  - ▶ 共**8位**同仁具ISO 27001 LA證照(網路組6位)
    - 2位**為教育機構資安驗證中心主導稽核員
    - 1位**為教育機構資安驗證中心稽核觀察員
    - 1位**為教育體系資安檢核技術服務中心稽核人員
- ▶ 提供「網站應用程式EVS弱點掃描平台」服務(成功大學)，並提醒連線單位對外服務網頁應定期排程掃描。

# 資安服務維運具體辦理事項

- 資安事件通報管理：連線單位發生資安事件30分鐘後，若尚未至通報平台完成通報程序，資安人員會**主動以LINE或打電話方式至連線單位提醒**。**今年度事件為32筆，超過30分鐘提醒通知共計24次。**
- 網站應用程式EVS弱點掃描平台：每半年掃描區網相關網站一次。
- 連線單位資安業務諮詢及到校輔導服務（因疫情因素改由其他方式協助）。
- 辦理資安教育訓練：ISMS文件製作、資通安全維護計畫撰寫、網站應用程式EVS弱點掃描平台、資安通報平台介紹、資通安全維護計畫實施情形實施情形線上填報教育訓練。
- 區網中心網頁維護：教育訓練資訊，並於每週四更新「TOP 500惡意IP位址網頁」。當接收到TACERT轉發「台灣電腦網路危機處理暨協調中心」資安訊息警訊時，若情資分享等級為WHITE(情資內容為可公開揭露之資訊)，會即時轉給連線單位，並公告於區網網頁之「最新消息」。**本年度共轉發48則資安情資給連線單位。**

## ➤ 連線服務

- 區網中心運作情形
- 創新服務
- 推動網路資訊應用環境之導入
- 教育訓練及推廣活動
- 年度計畫KPI辦理情形
- 綜合建議

## 區網中心運作情形(1/4)

- 每年召開**2次**連線學校管理會議
  1. 本年度已召開1次(8月25日、預計12月15日召開第二次)
  2. 8月25日出席率為**88%**(二個單位請假)
- 教育部所辦理之會議及活動(如管委會、技術小組會議) **100%參與**
- 有透過Smokeping對網路連線做監測，區網中心對臺北主節點電路妥善率達**99.92%**，對連線單位妥善率平均達**99.50%**以上

## 區網中心運作情形(2/4)

- 本年度辦理5場教育訓練，包含
  - ISMS文件製作(1場)
  - 資通安全維護計畫撰寫(1場)
  - 網站應用程式EVS弱點掃描平台(1場)
  - 資安通報平台介紹(1場次)
  - 資通安全維護計畫實施情形線上填報教育訓練(1場)
- 連線單位網管人員聯絡資訊至少每半年檢視更新一次(最近一次為9月1日)
- 年度營運計畫KPI除缺少召開一次連線學校管理會議外，其餘已全部達成。

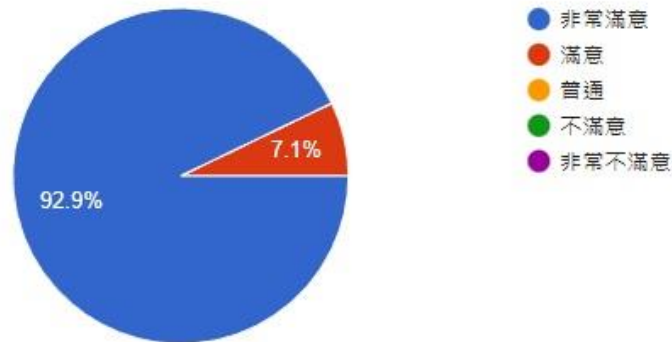
## 區網中心運作情形(3/4)

### ➤ 110年度連線單位服務滿意度報告(110年滿意度調查)

- 本年度共 **14** 個單位填寫問卷
- 教育訓練滿意度，**非常滿意達92.9%**
- 綜合整體服務的表現，本年度**非常滿意達100%**

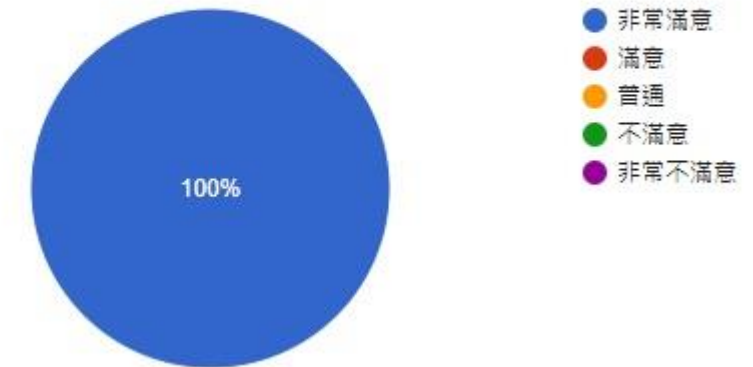
9. 對區網所舉辦之教育訓練或研討(習)課程，是否能符合貴校(單位)實務運作上的需求?

14 則回應



教育訓練滿意度

14 則回應



整體滿意度

## 區網中心運作情形(4/4)

- ▶ 基礎維運與資安人員計畫，教育部補助經費1,476,500元，至11月中旬執行率約**84%**。

經費項目	預算金額
人事費	1,143,693元
業務費	182,807元
設備費	150,000元
合計	1,476,500元



## 年度KPI辦理情形(1/2)

- 每年至少召開2次連線學校管理會議
  - 本年度已召開**1次**，**第二次召開時間預計為12月15日**
- 網路可用率達到99%以上
  - 對臺北主節點達**99.92%**，對臺南主節點(備援)達**99.27%**，對連線單位平均達**99.50%**以上
- 辦理至少5場教育訓練
  - 本年度辦理**5場**教育訓練
- 輔導至少5個高中職學校連線單位WWW向上集中至區網中心
  - 目前集中數量已達**10個**

## 年度KPI辦理情形(2/2)

- 加強推動連線單位IPv6網路環境建置，至少協助9個連線單位使用IPv6網路服務
  - 已有16個連線單位使用，僅剩1個單位未完成。
- 至少至連線單位到校服務10次，以協助解決問題
  - 本年度因疫情嚴峻，只能透過電話、LINE、遠端方式協助處理(共14次)。
- 本年度營運計畫KPI目前除缺少召開一次連線學校管理會議外，其餘已全部達成。

# 創新服務-到校輔導(1/3)

## ➤ 巡迴到校服務

- 組織輔導團隊，**巡迴至各連線單位**協助解決網路與資安問題，並做成輔導紀錄
- 每半年實施**乙**次，每次半天，可隨時至連線單位協助處理問題
- 本年度因疫情嚴峻，只能透過電話、**LINE**、遠端方式協助處理(共**14**次)。

# 創新服務-到校輔導(2/3)

The screenshots show a multi-part conversation:

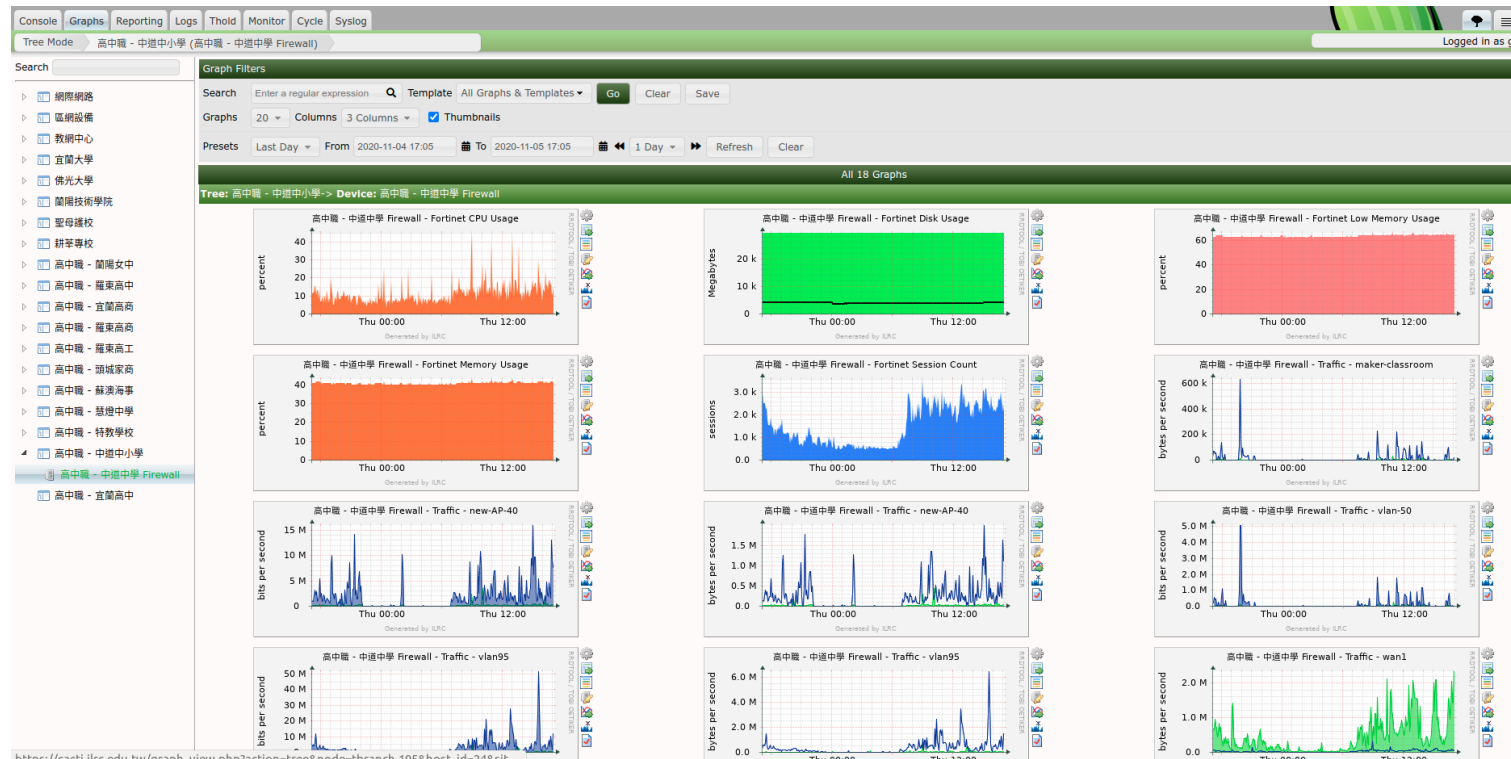
- Top Left:** A message from 'K...ag' to '主任好' (Principal Good) at 11:12 AM. A green bubble says: "evs平台 有一個學習系統 高風險4個 學校首頁跟生命學科中心今年都尚未掃描" (The evs platform has a learning system with 4 high-risk items. The school homepage and Life Science Center have not been scanned this year).
- Top Middle:** A message from '何...' at 2:33 PM: "你把資訊給大同" (Give the information to Datong). A response 'ok' is received at 2:33 PM. Another message at 2:33 PM asks: "IPV6要一起設定嗎 還是等這個好在設" (Should IPV6 be set together or wait until this is set?). A reply at 2:33 PM says: "我先給你資訊好了" (I'll give you the information first).
- Top Right:** A date separator for 2019.4.13. A green bubble contains a link: "【IFTT】 HITCON ZeroDay Disclosed 蘭陽女中 存在資料庫注入漏洞 - 高 <https://zeroday.hitcon.org/vulnerability/ZD-2019-00132> HITCON ZeroDay - 漏洞細... SQL Injection".
- Middle Left:** A screenshot of a scan report table. A message at 11:13 AM says: "學科中心的網站我等一下會移除因已經向上集中到國教署" (I will remove the website of the Life Science Center as it has been centralized to the National Education Commission). A follow-up message at 11:13 AM says: "學校首頁我等一下再申請風險掃描" (I will re-apply for a risk scan for the school homepage).
- Middle Middle:** A date separator for 7月13日 (July 13th). A message at 2:34 PM says: "你們的 2001:288:0:F:107 區往這邊2001:288:0:F:10". A response at 2:34 PM says: "好的, 我一起給大同" (Okay, I'll give it to Datong together).
- Middle Right:** A date separator for 7月28日 (July 28th). A message at 10:15 AM says: "主任抱歉假日打擾" (Principal, sorry for disturbing you on a holiday). A response at 10:26 AM says: "我有修正了, 不知道如何再測試看看有通過?" (I have corrected it, but I don't know how to test it again to see if it passes?). A reply at 9:03 PM says: "我們會再測試, 再跟主任回報" (We will test it again and report back to the principal).
- Bottom Middle:** A message at 11:03 AM says: "梁老師好, 貴校有資安預警通報待處理" (Hello Mr. Liang, your school has a security alert report to be processed). A response at 11:36 AM says: "我昨天有填了" (I filled it out yesterday). A follow-up message at 1:46 PM asks: "有上平台填報嗎?" (Did you report it on the platform?). A response at 1:48 PM shows a screenshot of a form.
- Bottom Right:** A message at 11:55 AM says: "要請組長上去排程掃描" (Please ask the group leader to schedule the scan). A response at 12:17 PM says: "好的, 感謝" (Okay, thank you).

## 創新服務-雲端伺服器服務(3/3)

- 區網中心提供連線單位**雲端伺服器服務**
  - 由區網中心建置VM主機( 透過本年度15萬元設備費，增購記憶體達512G )，提供連線單位使用
  - **DNS服務：8個**連線單位
  - **WWW服務：10個**連線單位
- 已提供1個連線單位使用備份服務(NAS由連線單位自備)

# 推動網路資訊應用環境之導入(1/2)

➤ 透過MRTG、Weathermap、Cacti、N-partner及Smokeping等軟體監控連線單位流量及線路穩定性





# 推動網路資訊應用環境之導入(2/2)

22

- 自行開發網路服務偵測系統
- 定時偵測連線單位網路服務



※主機服務狀態

目前第1/1頁 [首頁][前一頁][1][下一頁][尾頁]

服務名稱	狀態	最後檢查時間	主機異常時間
MRTG流量圖	on	2021-10-28 10:10:02	正常
私立中道國際中小學	on	2021-10-28 10:10:02	正常
私立慧燈中學	on	2021-10-28 10:10:01	正常
佛光大學	on	2021-10-28 10:10:01	正常
宜蘭大學	on	2021-10-28 10:10:02	正常
宜蘭高級中學	on	2021-10-28 10:10:02	正常
宜蘭特殊教育學校	on	2021-10-28 10:10:02	正常
宜蘭高商	on	2021-10-28 10:10:02	正常
宜蘭教網中心	on	2021-10-28 10:10:03	正常
宜蘭區網首頁	on	2021-10-28 10:10:03	正常
耕莘健康管理專科學校	on	2021-10-28 10:10:02	正常
聖母醫護管理專科學校	on	2021-10-28 10:10:02	正常
頭城家商	on	2021-10-28 10:10:02	正常
羅東高中	on	2021-10-28 10:10:02	正常
羅東高級工業學校	on	2021-10-28 10:10:02	正常
羅東高級商業職業學校	on	2021-10-28 10:10:01	正常
蘇澳高級海事水產職業學校	on	2021-10-28 10:10:02	正常
蘭陽女子高級中學	on	2021-10-28 10:10:01	正常
蘭陽技術學院	on	2021-10-28 10:10:01	正常

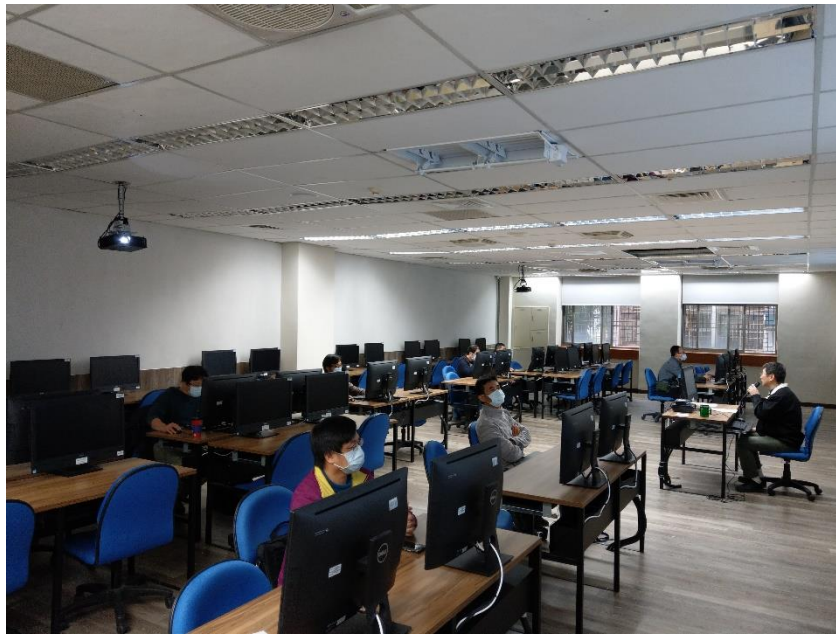
目前第1/1頁 [首頁][前一頁][1][下一頁][尾頁]



# 教育訓練及推廣活動(1/3)

日期	課程或活動名稱	時數
2021/10/27	資通安全維護計畫實施情形線上填報教育訓練	4
2021/08/25	資安通報平台介紹	1
2021/08/25	網站應用程式EVS弱點掃描平台介紹	1
2021/01/27	資通安全維護計畫撰寫	2
2021/01/27	ISMS文件製作	2

# 教育訓練及推廣活動(2/3)



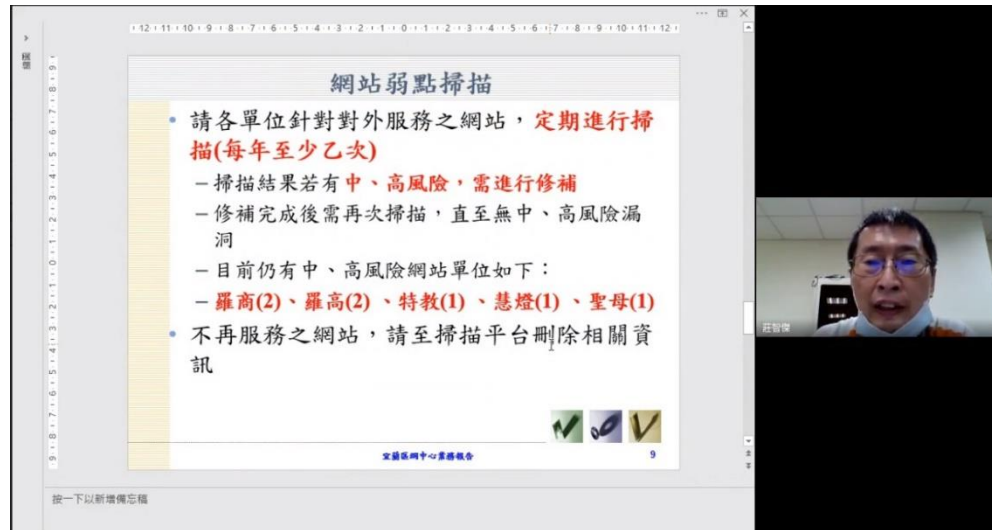
維護計畫撰寫

ISMS文件製作



# 教育訓練及推廣活動(3/3)

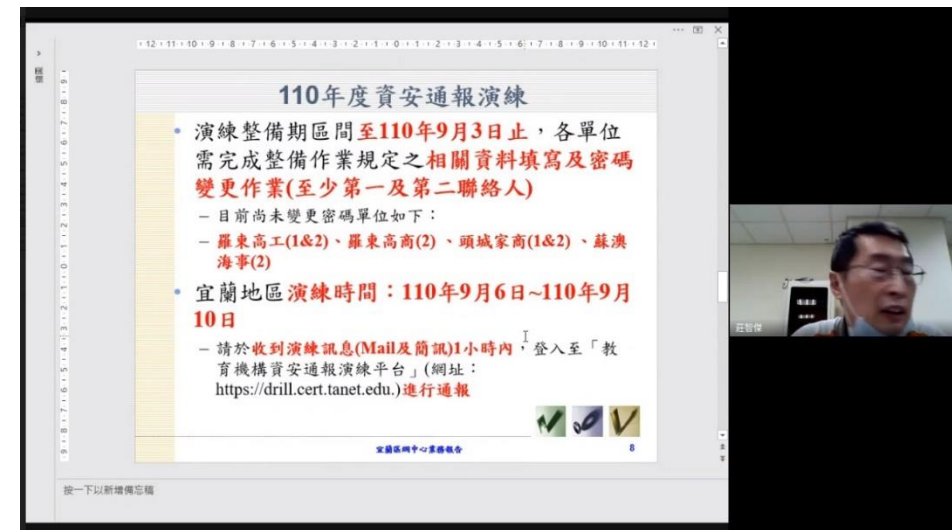
## EVS弱點掃描平台操作介紹



**網站弱點掃描**

- 請各單位針對對外服務之網站，**定期進行掃描(每年至少乙次)**
  - 掃描結果若有**中、高風險**，需進行修補
  - 修補完成後需再次掃描，直至無中、高風險漏洞
  - 目前仍有中、高風險網站單位如下：
    - 羅高(2)、羅高(2)、特教(1)、慈燈(1)、聖母(1)
- 不再服務之網站，請至掃描平台刪除相關資訊

按一下以新增備忘稿



**110年度資安通報演練**

- 演練整備期間**至110年9月3日止**，各單位需完成整備作業規定之**相關資料填寫及密碼變更作業(至少第一及第二聯絡人)**
  - 目前尚未變更密碼單位如下：
    - 羅東高工(1&2)、羅東高商(2)、頭城家商(1&2)、蘇澳海事(2)
- 宜蘭地區**演練時間：110年9月6日~110年9月10日**
  - 請於**收到演練訊息(Mail及簡訊)1小時內**，登入至「教育機構資安通報演練平台」(網址：<https://drill.cert.tanet.edu>)進行通報

按一下以新增備忘稿

## 資安通報平台介紹

## 綜合建議(1/5)

- 區網中心運作良好且均能達到鈞部及連線單位的要求
- 連線單位於連線會議及問卷調查時所提出之問題與回應
  - (連線單位)網管能力尚不足，人力不夠。
    - (區網回應)連線單位如遇問題，可透過LINE群組及電話告知區網中心，必要時可到現場協助處理。
  - (連線單位)協助整體網路頻寬提升，價格降價。
    - (區網回應)部內已協調全國統一價格。
  - (連線單位)虛擬機器的管理知識能力需加強。
    - (區網回應)明年度將於教育訓練課程中增設科目。

## 綜合建議(2/5)

### ➤ 去年度委員建議事項與回覆

- 目前高中職連線頻寬大部分皆為50Mbps，似乎頻寬有點過低，同時使用率亦較低，建議思考如何協助解決，以使高中職之網路使用能更順暢。

已於本年度協助有意願學校陸續提升

**16所學校僅剩3所頻寬低於100M(1所國立高職、2所私立高中)**

- IPv6之推動雖然有些困難，但建議將問題列出並協助其解決。

本年度已與各校連繫，目前除了耕莘專校(宜蘭校區)外，

所有連線單位均已完成IPv6連線。



## 綜合建議(3/5)

➤ DNS版本更新影響資安甚大，建議盡速協助連線單位完成。

國立高中職DNS已集中至區網中心，版本均維持最新。

➤ 受限於人力及經費等問題，自我研發之能力較受限，建議能引進其他區網已開發之系統，以服務連線單位。

建議導入其它區網中心研發的一些管理系統。

目前17個連線單位除縣網中心外，高中職佔多數(11所)。區網所提供之現有系統，連線單位回覆已符合所需。若連線單位有提出其他要求，再評估是否引進其他區網已開發之系統，以服務連線單位。

➤ 針對下年度之營運，將目標之KPI予以量化具體，以利執行及評估。

年度計畫KPI均已量化。

## 綜合建議(4/5)

- 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。  
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。

109年12月連線學校管理會議中，多數學校提出開設ISMS相關教育訓練課程。本年度教育訓練除資安通報平台及弱點掃描平台介紹外，主要針對國立高中職資通安全維護計畫及ISMS文件進行教育訓練。

資安通報平台及弱點掃描平台教育訓練會搭配實際上線操作。



## 綜合建議(5/5)

- 109年度KPI仍有部分指標未完成，請思索改善具體作為。  
去年簡報遺漏Cacti的KPI項目報告，目前已將Cacti教學融入日常的維護協助中，加強連線單位的觀念及操作認知。
- IPv6已列為高中職前瞻KPI，惟目前所轄各校之推動等仍未見成效，請分析遇到問題及研議未來改善作為。  
去年12月連線單位會議中討論各單位問題所在，並於今年協助各校完成IPv6相關細節設定及連線。



## ▶ 未來營運

- ▶ 創新服務目標與構想
- ▶ 網路管理營運方針
- ▶ 資安服務目標

## 創新服務目標與構想

- ▶ 因區網中心人員具有導入資訊安全ISMS之豐富輔導經驗，擬**提供高中職連線學校客製化ISMS文件**，以符合**資通安全管理法**相關規範。
- ▶ 配合教育部國教署高級中等學校以下學校核心系統向上集中政策，利用區網中心現有資源，**持續維護轄下所有國立高中職學校DNS、WWW主機**。

# 網路管理營運方針

- 持續維運網路，提供連線單位穩定之網路環境。
  - 透過相關流量、分析統計、監控軟體(如：Cacti、Smokeping、N-reporter)，作為網路狀況評估的依據，並在設備發生異常或中斷時發出警示信件通報，讓網路管理人員能夠在最短的時間內獲知訊息並針對該狀況進行處理。
- 持續維護轄下連線單位學校DNS、WWW主機。
- 辦理網路教育訓練，強化各連線單位網管人員的技能。
  - 於連線單位會議中確認需求。
- 持續提供連線單位網管業務諮詢及到校輔導服務。

# 資安服務目標

- 資安事件通報管理暨連線單位資安事件提醒告知。
  - 連線單位發生資安事件30分鐘後，若尚未至通報平台完成通報程序，資安人員會主動以Line或打電話方式至連線單位提醒。
- 定期掃描區網相關網站弱點。
  - 透過網站應用程式EVS弱點掃描平台定期掃描。
- 輔導連線單位維運ISMS管理制度。
- 辦理資安教育訓練。
  - 於連線單位會議中確認需求。
- 連線單位資安業務諮詢及到校輔導服務。



THANKS