# 臺灣學術網路(TANet)區域網路中心

# 115 年度基礎維運與資安人員計畫

申請單位：國立東華大學

區網名稱：花蓮區域網路中心

計畫主持人：陳偉銘 處長

中　華　民　國　１１４　年　１２　月　２　日

# 【目　　錄】

**壹、計畫基本項目 ..... 3**

一、計畫期程 ..... 3

二、計畫執行單位 ..... 3

**貳、計畫執行內容 ..... 3**

一、區域網路中心基本維運 ..... 3

(一)　現況說明(含網路架構圖) ..... 3

(二)　工作內容 ..... 7

(三)　辦理資訊推廣活動 ..... 15

(四)　特色服務 ..... 15

二、建構區網中心、連線單位及學校資通安全基本防護 ..... 18

(一)　現況說明(含網路架構圖) ..... 18

(二)　工作內容（含資安推廣服務） ..... 19

三、預期效益(KPI 指標) ..... 21

**參、經費需求 ..... 21**

# 壹、計畫基本項目

一、計畫期程

本計畫預定於 115 年 1 月 1 日起至 115 年 12 月 31 日止。

二、計畫執行單位

執行單位:花蓮區網中心(國立東華大學圖書資訊處)

# 貳、計畫執行內容

一、區域網路中心基本維運

(一) 現況說明(含網路架構圖)

台灣學術網路管理委員會第 16 次會議（84 年 12 月 19 日）通過國立東華大學為花蓮區域網路中心(試行)以來，本校即全力投入推廣 TANet 之使用與服務。經過一年多的努力之後，本區網中心無論在各項軟硬體建設，及對區內各級學校服務上，均有相當之成效，因此台灣學術網路管理委員會第 22 次會議（86 年 6 月 12 日），正式通過本校為花東區域網路中心。

本校對區網中心各項業務積極推動，對於 鈞部各項政策及 TANet 管理委員會與技術小組所決議之事項均配合辦理，且於 87 年辦理 TANET1998 研討會、91 年辦理 ICS2002 國際計算機會議、95 年辦理 TANET 2006(原花蓮教育大學)、101 年協辦第 30 屆區縣市網工作研討會、105 年辦理 TANET2016、106 年辦理 ACM-ICPC 國際大學生程式競賽初賽與區賽及 NCS2017 全國計算機會議研討會等諸多大型活動深獲好評。

東華大學計算機中心於 95 年 8 月更名為「計算機與網路中心」，並於 97 年 8 月與花蓮教育大學合校後更名為「資訊與網路中心」，因為本校圖書館與資網中心在 101 學年第 1 學期第 1 次校務會議通過合併的緣故， 102 年 2 月 1 日正式更名為「圖書資訊中心」，組織調整為「綜合業務組」、「網路管理組」、「校務系統組」、「數位資源組」、「圖資服務組」、「採訪編目組」等共 6 組。107 年 8 月 1 日「圖書資訊中心」更名為「圖書資訊處」，裁撤「數位資源組」組織異動為 5 組。花蓮區網中心業務主要是由網路管理組執行，未來一年本中心將秉持過去一貫服務之精神，維持轄下單位網路穩定與安全，並加強各項網路服務與研發創新服務。

1. 校園網路現狀：

本校目前共有壽豐、美崙及屏東三個校區，其中屏東校區係與國立海洋生物博物館合作，並由其管轄，美崙校區現已改為東華創新研究園區，壽豐校區則已整併為單一校區。

各校區內各大樓均有網路之節點，採用的網路佈線方式為：主幹以 48C Single Mode 光纖（Gigabit Ethernet）連接各建物，建築物內部則採用 UTP 配線方式。現行採用之主幹及使用者端網路架構，利於未來校園網路架構改變時，只需於各大樓配線中心機櫃處更新設備，並以跳線技術加以適當之跳線即可，不必再另行施工，非常具有彈性。

2. 與 TANet 連線狀況：

本校現以 10 Gigabit 頻寬連接 TANet，另以一路 Gigabit Ethernet 連接 TWAREN 骨幹設備。校內以一部 Cisco ASR 9010 透過 10G 線路連接校內三部 HPE 12508 至行政教學區、宿舍區及資訊中心。

配合教育部 400G 骨幹建置相關工作

(1) 機櫃位置調整：

於目前機櫃位置如照片一旁已進行清理，以釋出空間如照片二所示，用於擺放 400G 骨幹的新增設備機櫃。



照片一目前機櫃



照片二 400G 機櫃位置

(2) 電力系統規劃

電壓要求：

400G 骨幹設備預計使用 380V/220V 交流供電方式。

專用 UPS 配置：

配備骨幹專用 UPS，該設備可連接到配電室提供雙迴路電源，並確保有穩定的獨立電源可用於骨幹設備供電。

(3) 空調系統

空調部份採用中央空調並搭配 6 台大金吊隱式空調機。

目前已全面規劃了 400G 骨幹建置 所需的空間調整、電力規劃、以及空調系統等工作，目的是確保骨幹網路建置後的穩定運行與長期可用性。

轄下連線單位與頻寬：

目前仍連線的單位計有 15 個，圖三為現行網路架構圖，其中連線單位與連線方式、頻寬如下列說明：

(1) 東華大學 (10G 專線)

(2) 花蓮縣網中心 (40G 專線)

(3) 慈濟大學 (2G 專線)、慈濟科技大學 (1G 專線)

(4) 大漢技術學院 (1G 專線)

(5) 花蓮高工 (500M 光纖)

(6) 花蓮高中 (1G 光纖)

(7) 玉里高中 (500M 光纖)

(8) 花蓮高商 (300M 光纖)

(9) 花蓮女中 (500M 光纖)

(10) 花蓮高農 (500M 光纖)

(11) 花蓮特殊教育學校 (300M 光纖)

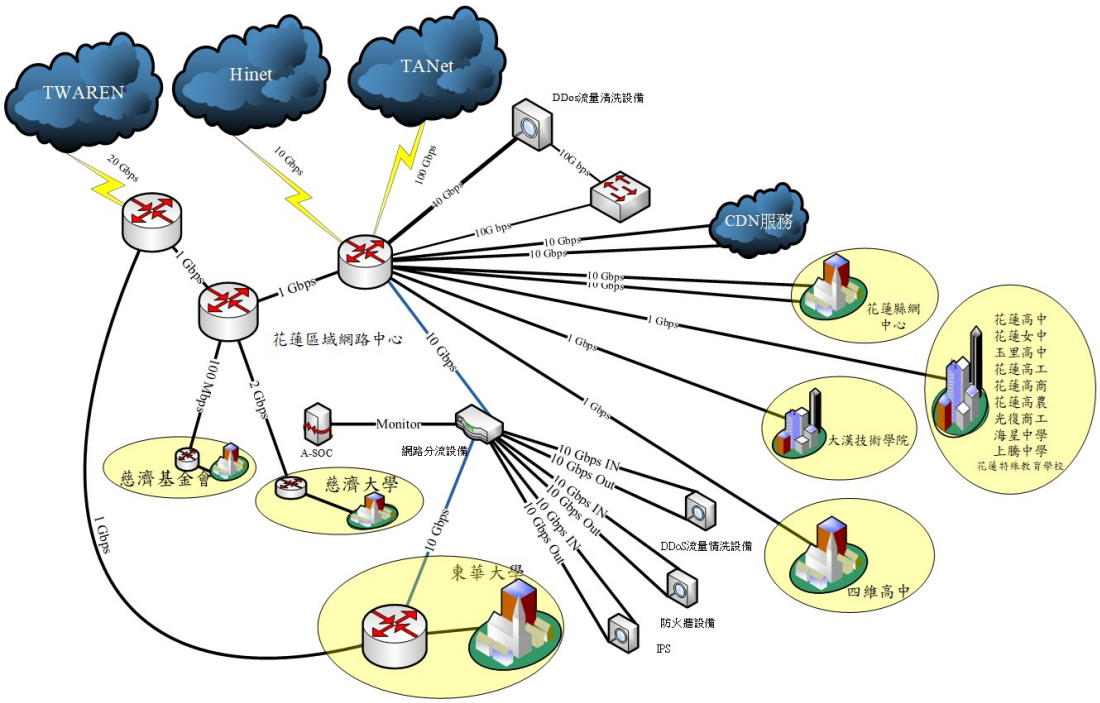
(12) 海星高中 (500M 光纖)

(13) 四維高中 (1G 光纖)

(14) 上騰中學 (500M 光纖)

(15) 光復商工 (0M 光纖)

花蓮區網中心 網路連線架構圖2024Q4




圖一、花蓮區網中心-東華大學網路連線架構圖

3. 電腦教室：

本中心現有電腦教室可舉辦各種研習課程：

(A) 壽豐校區有個人電腦教室 7 間：

◆理工二館大樓

2 間，每間 58 部，每部電腦均安裝 Microsoft Windows 作業系統，並搭配 MS Office，且可透過網路直接連上 Internet、具廣播教學及投影設備。

◆人社二館大樓

1 間，共 46 部，每部電腦均安裝 Microsoft Windows 作業系統，並搭配 MS Office，可透過網路直接連上 Internet、具廣播教學及投影設備。

◆花師教育學院大樓

2 間，每間 55 部，每部電腦均安裝 Microsoft Windows 作業系統，並搭配 MS Office，且可透過網路直接連上 Internet、具廣播教學及投影設備。

◆圖資處

2 間，資 PC1、資 PC2 總共有 120 部，每部電腦均安裝 Microsoft Windows 作業系統，並搭配 MS Office，且可透過網路直接連上 Internet、具廣播教學及投影設備。

(B) 視聽教室：

本校分別於 11 棟大樓共設有 29 間講堂或會議廳、演藝廳，可容納 300 人以上的演藝廳或講堂共 3 間，其中人社二館的演藝廳更可容納 700 人以上，而可容納 200~300 人的有 3 間，100~200 人的有 18 間，100 人以下的有 5 間。以上各活動場地均配備多媒體設備，並具有無線網路，方便舉辦各類大、中、小型研討會。

4. 主要 TANet 網路與資安設備：

(A) CISCO ASR 9010 二部。
(B) HP A12508 三部。
(C) Fortinet FG-1500D 一部。
(D) Palo Alto PA-5220 入侵偵防設備一部。
(E) Fortigate 3810A 防火牆一部
(F) IMPERVA SecureSphere X2510 網站應用程式防火牆一部。
(G) Gigamon GigaVUE-HC2 網路分流設備一部
(H) A10 TPS3030 DDoS 清洗設備一部
(I) N-Reporter 網路流量分析設備一部

5. 現有 TANet 網路服務系統：

| 項　目 | Domain Name：Port | IP Address | 使用限制 |
|---|---|---|---|
| **DNS** | dns.ndhu.edu.tw | 163.28.160.11 | 開放花蓮區網中心連線學校查詢 |
| **DNS** | dns2.ndhu.edu.tw | 134.208.10.11 | 開放花蓮區網中心連線學校查詢 |
| **BBS** | bbs.ndhu.edu.tw :23 | 134.208.10.240 | 身份確認之使用者 |

| | | | |
|---|---|---|---|
| **網頁弱點掃描系統** | evs.ncku.edu.tw | 163.28.114.8 | 開放花蓮區網中心有申請帳號的連線學校使用 |
| **WWW** | www.hdrc.edu.tw | 163.28.160.14 | 此為區網網站服務，無任何限制 |
| **異地備份服務** | - | 134.208.12.231 | 開放花蓮區網中心有申請帳號的連線學校使用 |
| **N-Reporter 網路流量分析系統** | - | 134.208.12.26 | 針對本區網各連線單位獨立開設帳號密碼 |
| **Cacti 網管系統** | - | 134.208.12.144 | 此為區網網站服務，無任何限制 |

## (二) 工作內容

### 1.網路管理

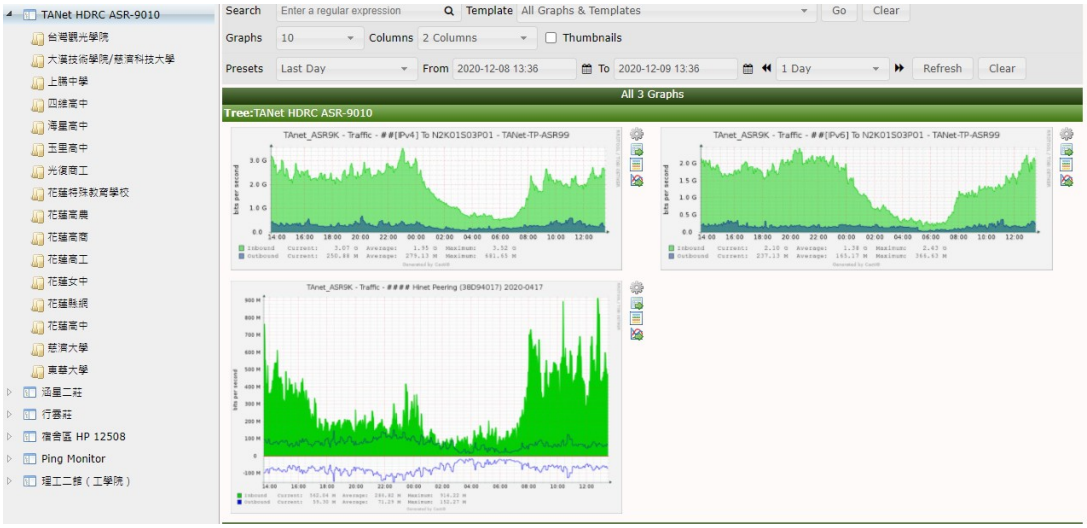
(1) 阻擋所有不正常流量

在 TANet 及 Hinet 的入口建置網路分流設備 GigaVUE-HC2，外面進來的流量會先進出 DDoS 清洗設備，然後再進出 IPS 設備，有效阻擋所有不正常流量。校內所有的 P2P 流量是由 IPS 設備進行阻擋，有效減少智財權侵權事件。

任何要進本區網中心－東華大學的流量，會先經過入侵偵防設備 Palo Alto PA-5220 及防火牆 Fortigate 3810A 的過濾。

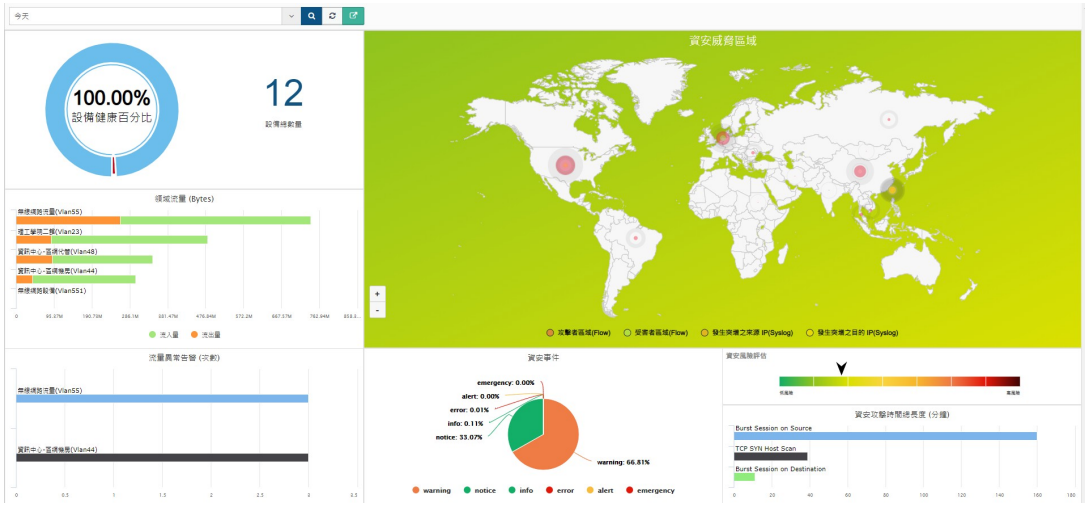
(2) 流量統計及異常分析

I. Cacti 網管系統是透過 WebUI 圖型化操作界面來進行設定管理,可以簡單快速的產生各種想要監控的物件資料，可以畫出容易閱讀的網路氣象圖。此系統並提供各式外掛套件及分享各大原廠設備的偵測模組（Template），不但增強 Cacti 原始程式碼的穩定性，也豐富了 Cacti 能夠擴充的資源。(詳如圖二)




(圖二、Cacti 網路流量統計圖)

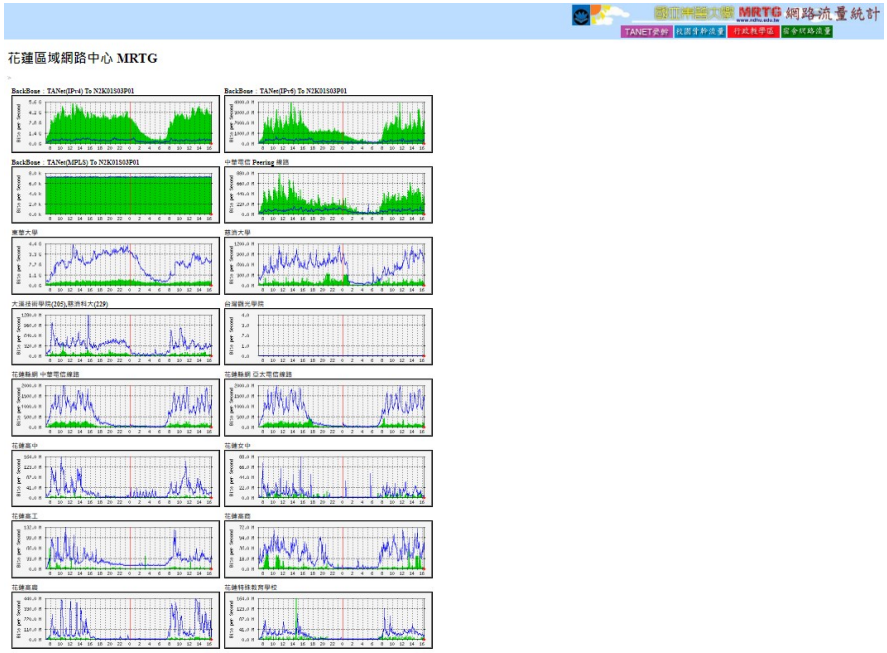
II. 透過 N-Reporter 網路流量分析報表軟體，收集來自 Router、IPS 及 FW 等設備的所有 log，以偵查來自於外部和內部威脅的情況，以及每個 IP、服務、單位、部門、使用者的網路用量，並統一提供即時或批次的報表分析。此系統同時針對本區網各連線單位獨立開設帳號密碼，使其能共享這套軟體的報表功能，如圖三所示。




(圖三、N-Reporter 流量分析圖)

III. 透過 MRTG，可觀察骨幹網路及連線單位的流量變化，作為 Cacti 的輔助使用。

流量統計相關資訊請參考 http://mrtg.ndhu.edu.tw。(詳如圖四)




(圖四、MRTG 網路流量統計圖)

(3) 資安事件檢舉處理機制

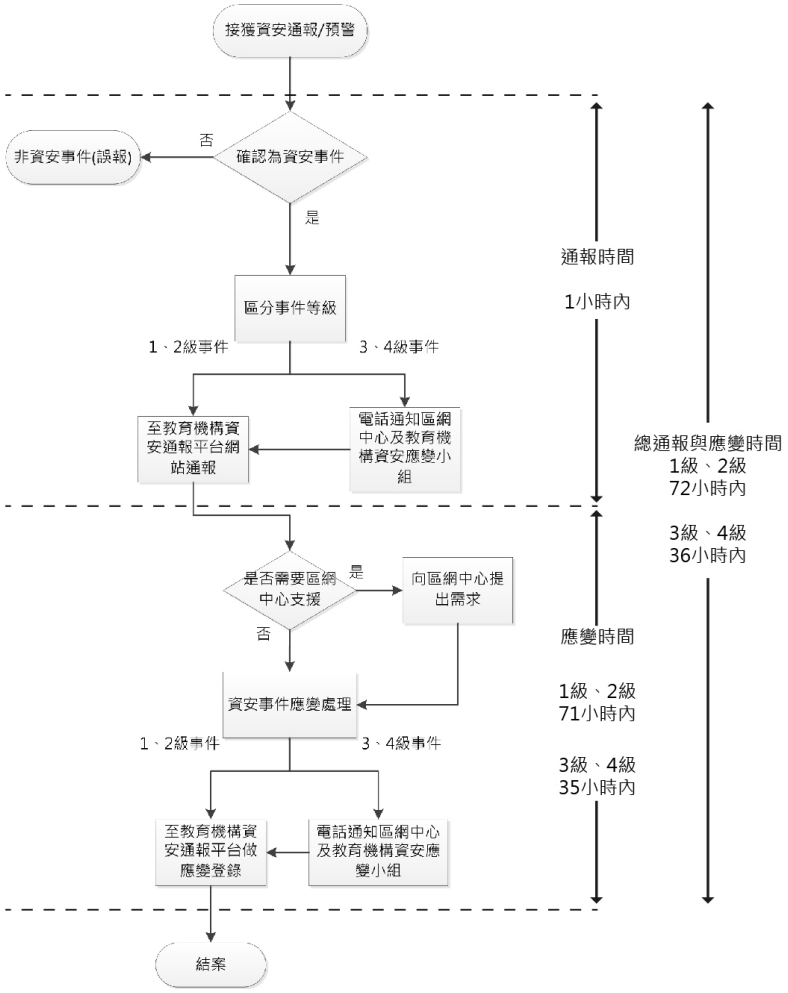
本區網於 104 年 7 月 29 日連線單位網路管理會 104 年第 1 次會議上決議，待完成事件通報後解鎖。會議上同時制定連線單位資安事件通報應變作業流程及花蓮區網中心資安事件通報應變審核流程，詳見附圖五、附圖六。

依據現行資通安全事件通報及應變辦法，知悉資通安全事件後，應於 1 小時內依主管機關指定之方式及對象，進行資通安全事件之通報。1、2 級事件於 8 小時內完成審核，3、4 級於 2 小時內完成審核作業。連線單位網路管理會 104 年第 1 次會議上制定連線單位資安事件通報應變作業流程及花蓮區網中心資安事件通報應變審核流程，詳見附圖五、附圖六。

如連線單位資安事件應變與處理時間偏長將分析具體案例，同時提供技術支援等等。

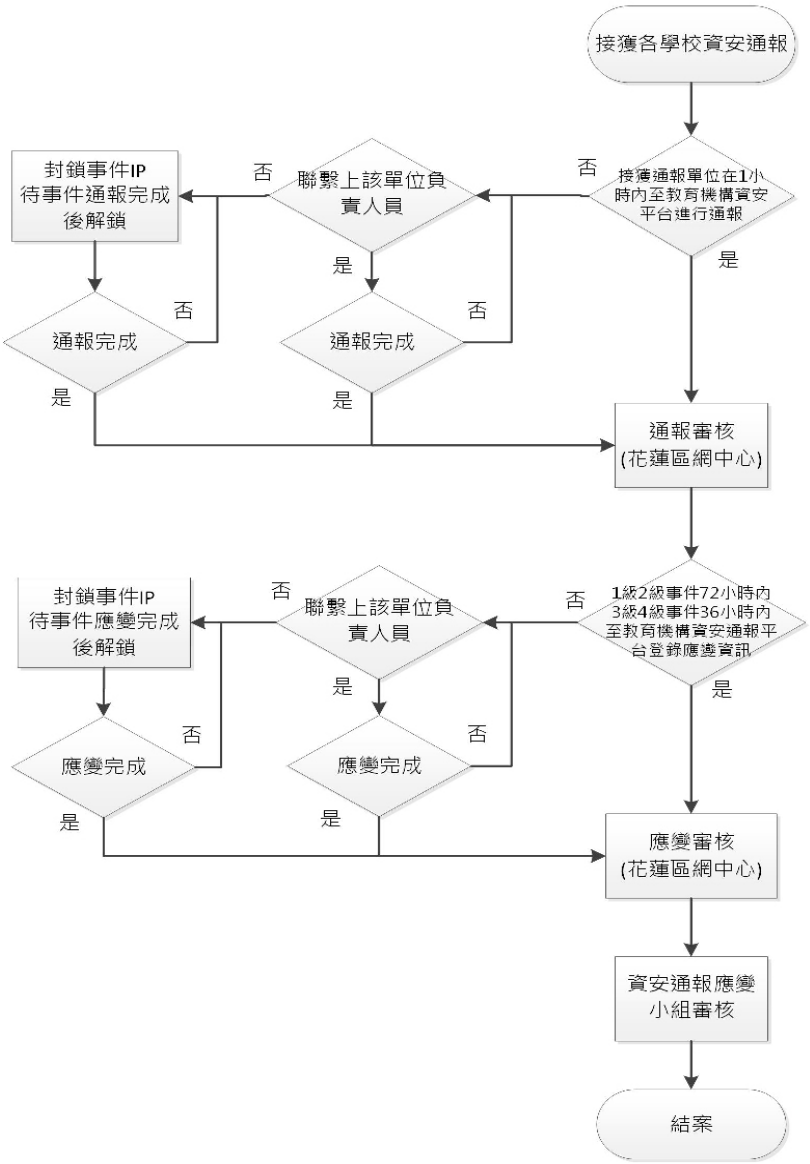
連線單位若於知悉資通安全事件後的 30 分鐘內未進行通報，將以電話方式聯繫該連線單位之資安通報聯絡人，提醒進行通報。以及每年配合教育部進行資安通報演練，以提高連線單位應變作業的熟悉度。

資訊安全事件通報應變作業流程




(圖五、資安事件通報應變作業流程圖)

花蓮區網中心資訊安全事件通報應變審核作業流程

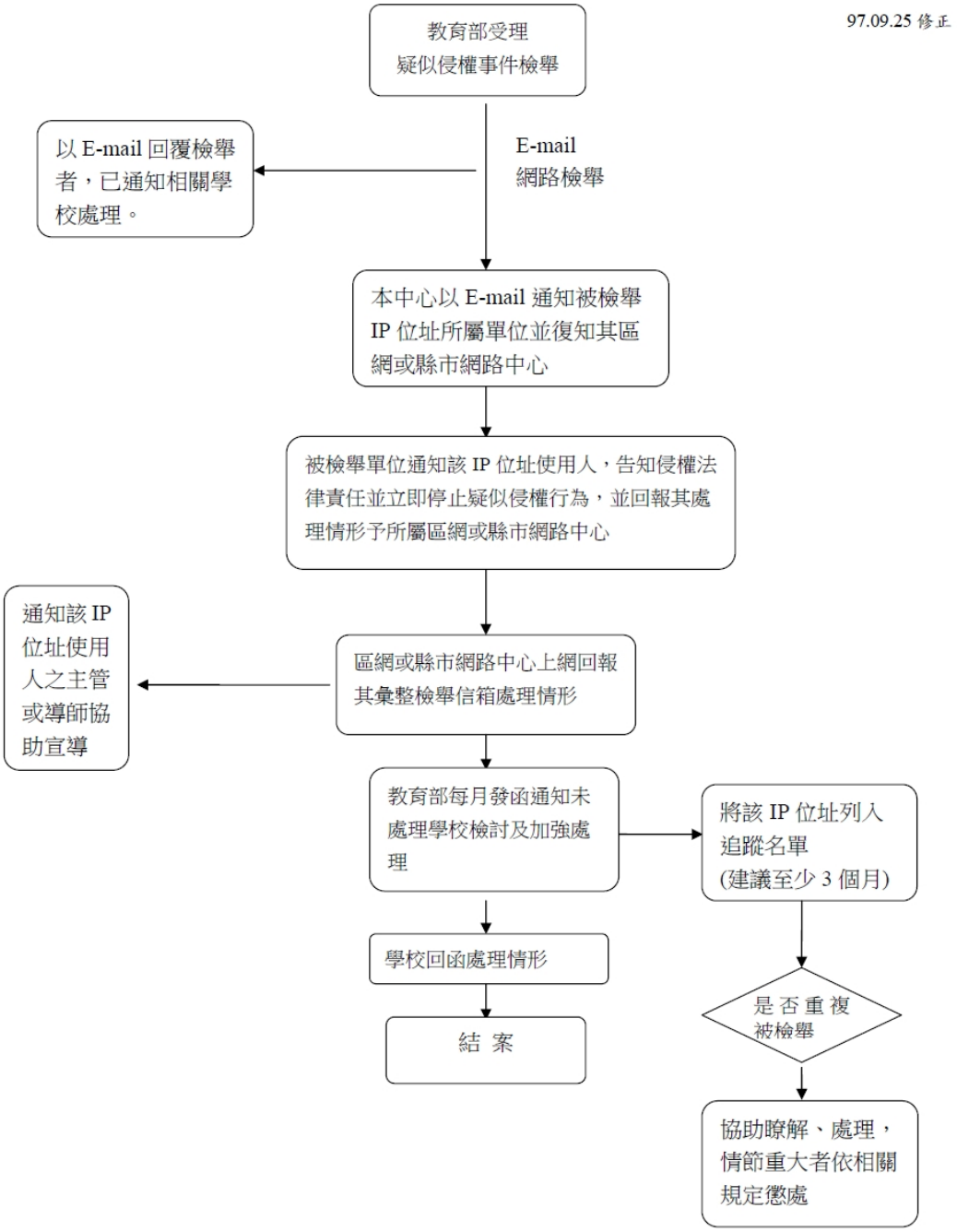



(圖六、資安事件通報應變審核流程圖)

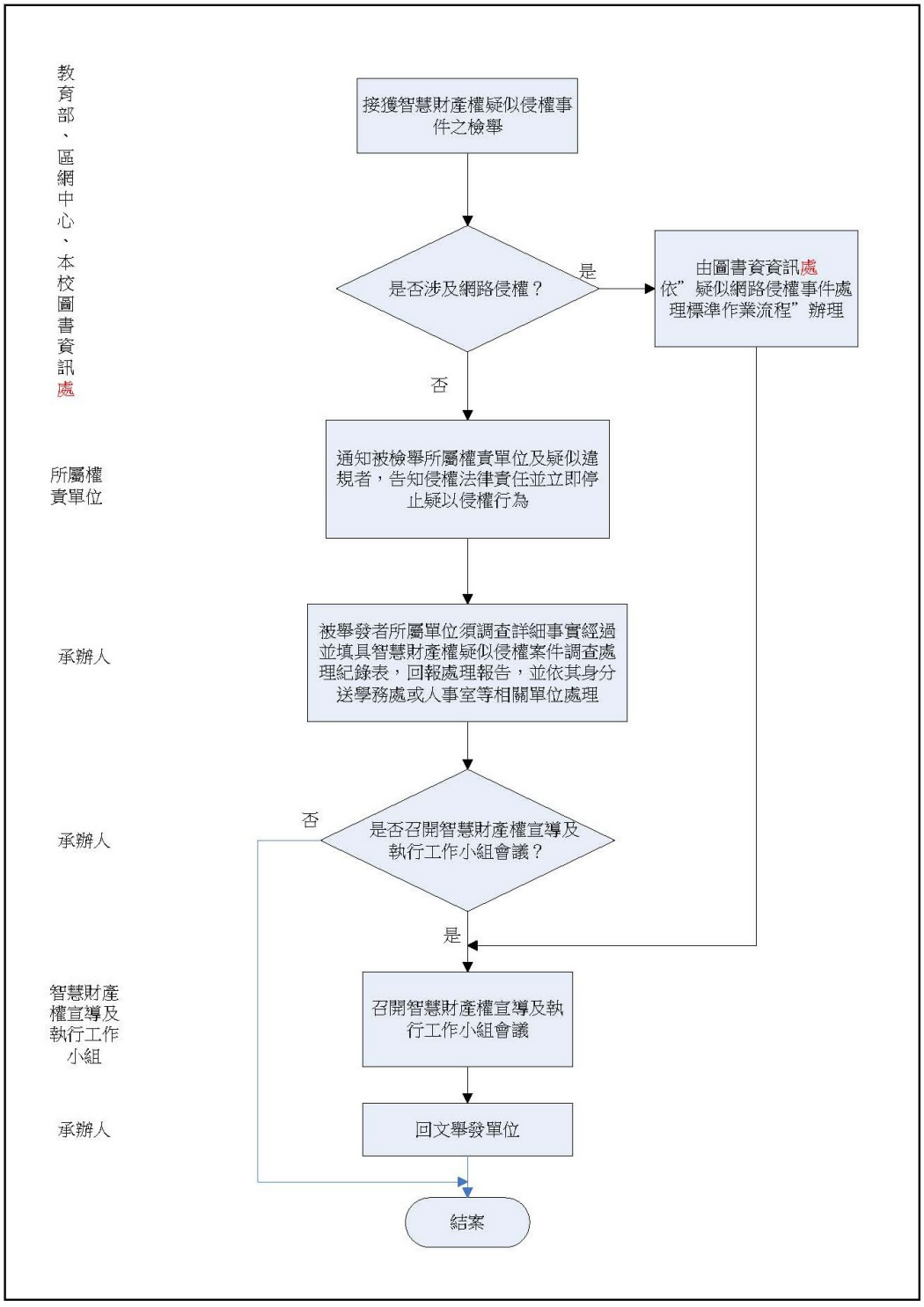
(4) 智財權檢舉案件處理

近年來由於智慧財產權侵權的問題日益嚴重，讓台灣學術網路成為侵權的工具之一，本中心配合教育部擬定台灣學術網路智慧財產權疑似侵權處理程序，如圖七所示，進行相關的處理及回報。本中心在接獲教育部轉發之檢舉信後，於 5 個工作日封鎖疑似侵權電腦使用之 IP，並於網路上公告封鎖之 IP，接

著通知該 IP 使用者所屬單位，請使用者至本中心釐清責任，如屬實將依規定參加乙次智財權講習及停止網路使用權一學年。本中心主張教育單位應該以教育使用者正確的觀念為優先，所以特別規範針對違規的使用者必須參加智慧財產權講習，重新建立正確智財權觀念。本中心違反智財權處理流程如圖八所示。




(圖七、台灣學術網路智慧財產權疑似侵權處理程序)




(圖八、花蓮區網中心-東華大學處理疑似侵犯智財權流程)

## 2.加強與連線學校的互動

本校地處花蓮縣壽豐鄉，對連線學校而言，路途較為遙遠，為提高本區網中心連線單位網路管理會出席率，規劃每年召開的 2 次連線單位會議將於花蓮市區協商有意願提供場地的連線學校舉辦，這樣一來，可節省連線單位至開會地點的路程與時間，藉此提高與會的出席率，及加強與各連線單位的互動。

針對會議出席率低的問題，將通過調整會議時間至非教學高峰期。同時考慮以混合線上及實體方式召開，提升靈活性及參與率。平時透過郵件群組 hdrc@mail.ndhu.edu.tw 及 line 群組與轄下連線單位快速互動，區網中心有任何訊息或通知，均是利用郵件群組與 line 群組快速傳達至各成員，包含部裏政策、資安訊息、網路與資安技術等等。

因近年疫情影響，不便前往連線學校檢視環境及設備，也使用電話或線上會議方式進行討論，並提供相關建議及經驗給連線學校。本中心設置 24 小時緊急聯絡電話：03-8906723，會轉接至值班人員手機，可供連線學校於非上班時間，遇到緊急事件時聯繫使用。

## 3.對連線單位協調及提供諮詢、服務

本區網中心除定期召開花蓮區網中心管理會外，平時與各連線學校窗口負責人，保持電話與 E-mail 聯繫，轉知教育部各項政令，並接受各項網路故障申告，並且本中心網路維運人員，於發現網路有任何異常狀況時，也會於第一時間主動通知該校負責人，進行故障排除及處理教育部轉知之智財權及網路危害事件，為了提供各校更多的服務與資源共享，本中心建置了花蓮區網中心網站 http://www.hdrc.edu.tw/提供交流，如圖九所示，另外除了教育訓練外，我們也提供連線單位 DNS 代管、伺服器與網路設備代管、異地備援備份、DDoS 流量清洗服務等各項網路服務。




(圖九、花蓮區網中心網站)

4.業務永續運作計畫演練

每年會辦理業務永續運作計畫演練，因資安事件的發生多會伴隨不同情況，因此將以複合式情境作為演練項目，以確保當關鍵業務同時遭受多種情景、設備故障、災難事件而中斷時，能以迅速、有效的方法回復正常運作。

## (三) 辦理資訊推廣活動

本中心於本年度預定辦理至少 6 場以上資訊推廣活動，其中包含資通安全、網路技術、智慧財產權及個資保護等。我們將廣邀相關專家學者，為花蓮地區的 TANet 成員提供相關資訊教育訓練。

## (四) 特色服務

1. 規劃引進區網其他學校的資源來強化服務，學習其他區網的長處，服務轄下連線單位。
2. DDoS 流量清洗設備已建置完成，放置在區網端口，提供花蓮區網連線學校或單位 DDoS 攻擊清洗功能，以提昇資安保護層級，及保護花蓮區網整體網路運作安全。

   持續與連線單位推廣本區網 DDoS 流量清洗服務。
3. 提供 Cacti 流量監控網管系統

   Cacti 是個強大的流量統計圖表繪製工具，亦可說是進化版的 MRTG 軟體，在 Cacti 中新增偵測節點及建立偵測介面的操作，都可以透過 Web 連線方式進行維護及管理工作，比起傳統 MRTG 需要登入主機編修相關設定檔案文件，更容易讓網管人員學習上手。只要瞭解幾個 Console 介面的功能後，就可以完成基本的設備效能及流量偵測工作。

   使用此套系統，可讓轄下連線單位更容易使用與監控網路流量。
4. 提供 N-Reporter 網路流量分析報表軟體，並為各連線單位獨立開設使用帳密，使其可產出即時或批次的詳細流量分析報告，有助於對網路異常流量的分析與了解。
5. 持續推動區網主機代管服務，協助轄下單位建置更穩定的應用服務系統。
6. 到府服務

   由於花蓮民風淳樸保守，連線單位往往有困難也不想麻煩別人。未來將主動詢問連線單位的需求，以協助其建置系統或設定 IPv6，幫忙安裝網路監測軟體、提供技術諮詢及協助改善網路運作效能、排除資安技術問題等等，加強轄下連線單位網管與資安的防護能力。並安排時間到連線學校訪視。
7. 提供弱點掃描服務

   將新版免費弱點掃描軟體打包成一個套件，提供給有興趣安裝的連線單位，或者本區網亦可派人到連線單位幫其安裝。若是連線學校無法提供設備安裝，但卻有

弱點掃描需求者，我們亦可攜帶裝有弱點掃描軟體的筆電，到該連線單位協助其進行重要系統的弱點掃描。

8. 與漫遊中心合作，在花蓮區網中心打造第二伺服器據點

配合教育部 104 年初 TANet 與 iTaiwan 雙向漫遊開通互連的政策本校全面開放 TANetRoaming 的 WiFi 熱點，以方便他校的使用者得以使用本校的所有無線基地台，並繼續推動國際漫遊 Eduroam，TANet 無線網路漫遊交換中心已移至國立東華大學，並已建置完成，宜蘭大學為備援。

9. 建置區網 LINE 群組

(1) 透過 LINE 的聯繫可更迅速交換訊息及提供服務，當區網網路出現狀況時，也提供另一個可以聯繫的管道。

(2) 訊息傳遞更為迅速、即時。

10.實施遠端服務

(1)為協助連線單位更即時的服務，本區網設計 Google 表單詢問各連線單位的需求，配合其時間，派員到點服務，或以線上方式、通話方式遠端協助連線單位。

(2)為協助連線單位 IPv6 及 Eduroam 之建置，與連線單位預約時間將派員至該連線單位協助檢視建置之設備及環境。

(3)針對未完成 Eduroam 建置的學校，已納入觀察名單，並計劃逐步輔　導其實施，確保滿足教育部需求的同時提升學校使用便利性。

11.成立區網主機與設備代管區

(1) 提供連線單位放置伺服器或網路設備在本區網機房。

(2) 提供慈濟大學「校務系統主機異地備援服務」及「網路設備與主機寄放服務」。

12.異地備份服務

(1) 目前本區網有一套網路儲存系統(48TB)。

(2) 110 年購入一台 NAS，112 年購入網路儲存系統及 2 台 10G Switch。

(3) 本區網於 111 年與桃園區網(中央大學)簽訂異地備份，為符合異 地備份原則，雙方互惠建置 20T 空間，預計 114 年使用率會持續成長。

(4) 提供區網異地備份服務

區網可使用 SFTP、RSYNC、NFS 等方式進行異地備份服務。

使用 Synology NAS 備份工具與桃園區網進行合作。

花蓮、宜蘭、台東和桃園區網均以上述方式完成異地備份工作。

花蓮、宜蘭(主機代管，宜蘭區網自購 NAS)、台東區網均以 RSYNC 完成異地備份工作。

(5) 提供連線單位異地備份服務

連線單位可使用 SFTP 、RSYNC、NFS 進行異地備份服務。 每個單位提供 2TB 空間，視用量調整增加。

目前已有慈濟大學、花蓮縣網中心、花蓮高商、花蓮高工申請使用。備份空間使用率：慈濟大學使用率為 8.4% (1T 使用 84G)、花蓮縣網使用率為 80% (2.5T 使用 2T)、花蓮高商使用率為 28% (2T 使用 568G)、花蓮高工使用率為 11% (2T 使用 229G)及大漢技術學院 76%(2.5T 使用 1.9T)。持續提供異地備份服務給連線單位申請及使用，預計 114 年之使用率會漸進的增長，若連線單位欲增加備份空間，將視用量再進行調整。

(6) 提供海洋大學異地備份服務，備份空間使用率為 38%(2T 使用 761G)。

13.泛太平洋聯盟圖書資訊服務互惠協議

由東部 7 所大學共同訂定，分別為宜蘭大學、佛光大學、東華大學、慈濟大學、台東大學、海洋大學、淡江大學。

共用圖書、資訊資源，以合作、共利方式提升圖書資訊服務品質。

資訊服務部份，包含資料異地備分、ISMS 資安內稽支援、DNS 異地備援機制等。

14.提供轄下單位 DNS 相關服務

(1) 花蓮縣網中心 DNS 備援服務。

(2) 玉里高中、花蓮高農、花蓮高工、花蓮高中、花蓮女中 DNS 代管服務。

(3) 協助連線學校 DNS 相關設定。

15.全校建置 SSID 為 TANet Roaming 及 Eduroam 的 WiFi 熱點

方便他校訪客可以透過本校使用無線網路漫遊。

16.設備

因應轄下連線單位向上集中之服務，更新下列設備：2U 機架式伺服器，使用共約購入設備。更新機架式伺服器以提供向上集中服務、運作網頁及 DNS。

17.新增區與網站相關內容

(1) 新增影音學習專區，將近期花蓮區網舉辦過之研習，經過講師核可後錄影並剪輯內容，放上區網網站供使用者學習與複習，影片未來會依使用者需求持續增加。

(2) 增加花蓮區網問題 QA 專區，提供連線學校基本問題排除。

(3) 花蓮區網為提供轄下連線單位更好的服務，除了可撥打窗口電話與緊急電話外，另可填寫線上問題諮詢與服務申請表。

18.骨幹基礎環境、機房

(1) 113 年本區網骨幹基礎環境之妥善率為 99.95%，本區網於今年 4 月 3 日、4 月 23 日因地震發生 3 次連線中斷共 247 分鐘，第一次 4 月 3 日地震因為無法進入現場故中斷連線時間拉長至 177 分鐘，第二次及第三次地震因 100G SMR 電池老化負載時間僅 10 分鐘左右，其維護廠商已於 7 月 17 日更換電池。

(2) 國家高速網路與計算中心例行檢查均無異常，機房溫度及電力均正常。

(3) 114 年持續保持骨幹基礎環境，機房、設備、電力系統正常運行。

19.系統使用性

本區網 TANet 骨幹維運可用性達 99.6%以上，確保本校核心系統資訊機房維運服務達全年上班時間 99.6%以上之可用性，並確保因資通安全事件、異常事件、其他安全事故造成系統、主機異常而中斷營運服務之情事，每年不得超過 8 次、每次最長不得超過 4 小時。

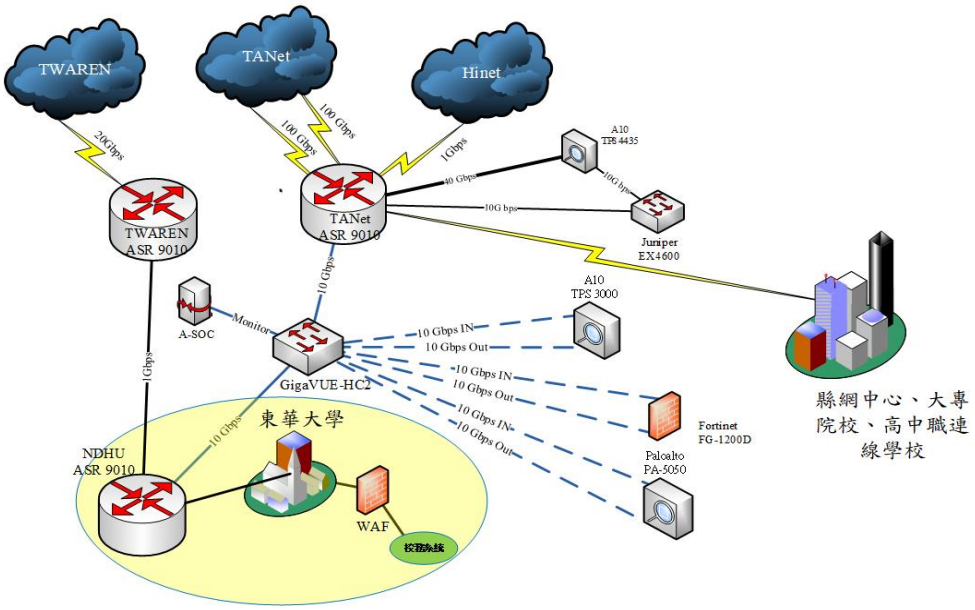
## 二、建構區網中心、連線單位及學校資通安全基本防護

### (一) 現況說明(含網路架構圖)

#### 1. 阻擋所有不正常的流量

本區網中心為防止學生侵犯智財權及提昇資安層級，特別在 TANet 及 Hinet 的入口建置資安設備 Fortigate FG-1500D、A10 TPS 3000 DDoS 攻擊清洗設備及 Palo Alto PA-5220，校內所有的 P2P 流量是由 Palo Alto 設備進行阻擋，有效減少智財權侵權事件。而任何要進本區網中心－東華大學的流量，會先經過入侵偵防設備 Palo Alto PA-5220 及防火牆 Fortigate 3810A 的過濾，因此，本區網整個的資安防護網，可算是相對的健全，資安防護架構圖如圖十所示。

花蓮區網中心資安防護網路架構圖




(圖十、資安防護網路架構)

### 2. 建置網頁弱點掃描系統

為協助建立長期營運機制，使連線單位有穩定的、可靠的監測工具，本中心使用由成大資通安全中心提供，於 107 年 5 月建置完成之「教育單位弱點檢測平台」。本中心提供入口網頁供連線單位申請掃描服務，網址為 https://evs.ncku.edu.tw/ 如圖十一所示，並新增弱點掃描 QA 專區於花蓮區網網頁中。




(圖十一、教育單位弱點檢測平台)

## (二) 工作內容（含資安推廣服務）

為提昇所屬連線單位落實資訊安全管理系統的有效性，本區網中心將提供資安諮詢服務，協助所屬連線單位建置資通安全基本防護工作，提供資通安全技術服務，協助區網及所屬連線單位進行網站弱點掃描及資安相關事宜。詳細工作如下說明：

### 1. 資安諮詢服務

(1) 持續維護與更新花蓮區網中心網頁問題集專區，提供連線單位基礎網管相關的問題解決方式，以及提供資安相關訊息、線上課程活動等訊息。

(2) 於花蓮區網中建置問題諮詢回報表單，提供多元的諮詢方式。

(3) 因連線單位多為高中，高中老師多為兼職，因此連線單位人員會不定期更動，區網將定期向連線單位更新人員資訊，並於區網網頁中進行更新。

### 2. 資安相關服務

(1) 派員協助連線單位 ISMS 稽核業務或依連線單位需求邀請專家學者。

(2) 與各連線單位分享資通安全管理法最新相關訊息，提供資安、個資管理之經驗。

(3) 提升連線單位資安防護，協助連線學校安裝弱點掃描系統或開放防火牆讓本區網協助掃描，並於完成後提供弱點分析與建議，及辦理相關教育訓練。

(4) DDoS 清洗服務，提供連線單位申請，改接線路至 DDoS 保護設備，啟動流量分析及學習流量指標,設置系統/服務流量監控樣板,啟動 DDoS 動態防禦政策。

(5) 辦理 6 場以上網路或資安相關之教育訓練，詢問連線單位的需求，依照其需求找尋講師，以及提供相關教育訓練、研討會、課程資訊。

(6) 轉知相關單位所辦理之研討會、課程資訊（例如教育部、TACERT、區網、大學等等），以提供更多的管道給連線單位參與。

(7) 持續提供連線單位(玉里高中、花蓮高農、花蓮高工、花蓮高中、花蓮女中 DNS 代管服務及相關協助。

(8) 持續協助 IPv6 之建置，給予適當建議及協助(例如：檢視環境、設備、提供建置之經驗)。

3. 專職人員

為使區網中心、連線單位及學校資通安全基本防護工作正常運作，本中心需四位專職人員，一位負責區網的網路維運，一位負責資安業務，一位負責雲端服務及一位教學資訊人力，其工作包含：

| 人力類別 | 服務內容 |
|---|---|
| **網管人力** | •協助 TANet 區網維運計畫執行<br>•負責花蓮區域網路的正常維運及故障排除<br>•協助舉辦花蓮區網中心研討會<br>•花蓮區網中心網頁維護管理<br>•協助花蓮區網中心報名網站管理與維護<br>•支援花蓮區網中心其他交辦事項 |
| **資安人力** | •花蓮區網中心資安業務處理<br>•資通安全專區與個資專區網頁維護管理<br>•辦理連線單位資安與個資教育訓練<br>•協助連線單位資安與個資內稽作業<br>•執行區網中心滿意度調查作業<br>•協助區網連線單位資安通報演練<br>•資安相關政策宣導及推廣<br>•辦理花蓮區網管理會會議<br>•支援花蓮區網中心其他交辦事項 |
| **雲端服務人力** | •依連線單位需求提供雲端基礎維運與管理教育訓練<br>•配合資安人力，進行雲端環境的弱點掃描與安全性分析<br>•協助連線單位雲端平台操作技術諮詢與問題排解 |

| | |
|---|---|
| | •協助連線單位提供雲端資源的應用或資料備援等<br>•協助連線單位提供資安與雲端服務的教育訓練<br>•資安相關政策宣導及推廣<br>•辦理花蓮區網管理會會議<br>•支援花蓮區網中心其他交辦事項 |
| **教學資訊人力** | •定期辦理資通安全或數位學習技術的教育訓練<br>•協助連線單位推動遠距教學，並提供相關的經驗及技術<br>•根據連線單位需求提供遠端教學相關技術支援<br>•資安相關政策宣導及推廣<br>•辦理花蓮區網管理會議<br>•支援花蓮區網中心其他交辦事項 |

## 三、預期效益(KPI 指標)

1. 預計完成花蓮區網內 2 間學校申請使用 DDoS 流量清洗設備服務。
2. 規劃提供到校服務或遠端技術支援至 5 所學校。
3. 預期協助 5 所連線學校進行 DNS 代管服務，包括異常處理與設定調整等工作。
4. 計畫舉辦至少 6 場資訊與資安推廣活動，其中包含一場實務操作課程。
5. 預計參與教育訓練的總人次達 200 人次以上。
6. 為所有連線單位提供到校或遠端技術支援，檢視其 IPv6 網路環境。
7. 至 7 所高中職及大專院校，檢視其 Eduroam 環境。
8. 預期協助 1 所連線學校建置並完善 IPv6 網路環境。
9. 召開 2 次區網管理會議。
10. 區網會議出席率目標達 80%（至少 12 所連線單位派員參與）。
11. 預計為 2 至 3 所連線學校提供弱點掃描服務，並提供詳細分析報告與建議。
12. 定期檢視與更新連線單位的基礎資料，全年完成 2 次聯絡資訊的更新作業。
13. 持續為 3 所連線學校提供異地備份服務，並確保其穩定運作。
14. 分享 5 場資安相關研討會或講座資訊予連線學校參考。
15. 確保連線學校網路服務妥善率及骨幹基礎設備的妥善率維持在 90%以上。

## 參、經費需求