

花蓮區域網路中心

「104 年度花蓮區域網路中心基礎維運 與資安人員計畫」

103 年 11 月 30 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	13
(四) 特色服務	14
二、建構區網中心、連線單位及學校資通安全基本防護	15
(一) 現況說明(含網路架構圖)	15
(二) 工作內容（含資安推廣服務）	17
三、預期效益(KPI 指標)	18
參、經費需求	19

壹、計畫基本項目

一、計畫期程

本計畫預定於 104 年 1 月 1 日起至 104 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中心)

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，及對區內各級學校之服務上，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。

本校對區網中心之各項業務積極推動，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等深獲好評。

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已經在 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」等共六組。花蓮區網中心之業務技術部份主要是由網路管理組執行，行政部份則由數位資源組負責推行，未來一年本中心將秉持過去一貫服務之精神，維持轄下單位之網路穩定與安全，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（100BaseT）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：

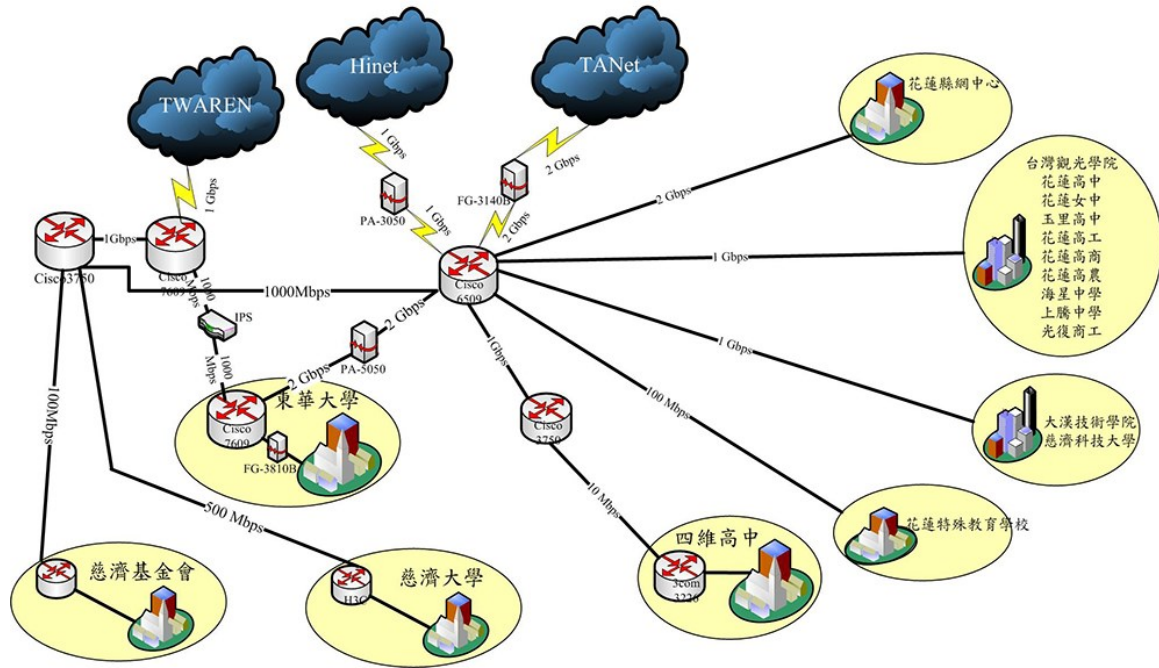
本校現以 Cisco 6509 透過二路 Gigabit Ethernet 連接 TANet，另以 Cisco 7609 經由一路 Gigabit Ethernet 連接 TWAREN 骨幹設備。壽豐校區分別以 2 部 H3C 12508 及 1 部 H3C 9512 連接至行政教學區、宿舍區、及圖資中心 B 棟。

3. 轄下連線單位與頻寬：

目前仍連線的單位計有 17 個，圖一為現行網路架構圖，其中連線單位與連線方式、頻寬如下列說明：

- (1) 東華大學 (2G 專線)
- (2) 花蓮縣網中心 (2G 專線)
- (3) 慈濟大學(500M)
- (4) 慈濟技術學院 (300M 專線)
- (5) 大漢技術學院 (200M 專線)
- (6) 台灣觀光學院 (50M 專線)
- (7) 花蓮高工(50M)
- (8) 花蓮高中(50M)
- (9) 玉里高中(50M)
- (10) 花蓮高商(50M)
- (11) 花蓮女中(50M)
- (12) 花蓮高農(50M)
- (13) 花蓮特殊教育學校(50M)
- (14) 海星高中(50M)
- (15) 四維高中(50M)
- (16) 上騰中學(50M)
- (17) 光復商工(ADSL)

花蓮區網中心 網路連線架構圖 (2015Q4)



圖一、花蓮區網中心-東華大學網路連線架構圖

4. 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，每間為 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，為 46 部，每部電腦均安裝 Microsoft Windows 作業系統，並搭配 MS Office，並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，每間為 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。

圖資中心-- 2 間，資 PC1、資 PC2 分別為 61 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。

5. 主要 TANet 網路設備：

- (A) 本中心現有 CISCO 7609 二部及 6509、7513、1010 各一部。
- (B) H3C 12508 二部。
- (C) H3C 9512 一部。
- (D) Radware DP-3020、DP-3016 入侵偵防設備各一部。
- (E) Palo Alto PA-3050 入侵偵防設備一部。

6. 現有 TANet 網路服務系統：

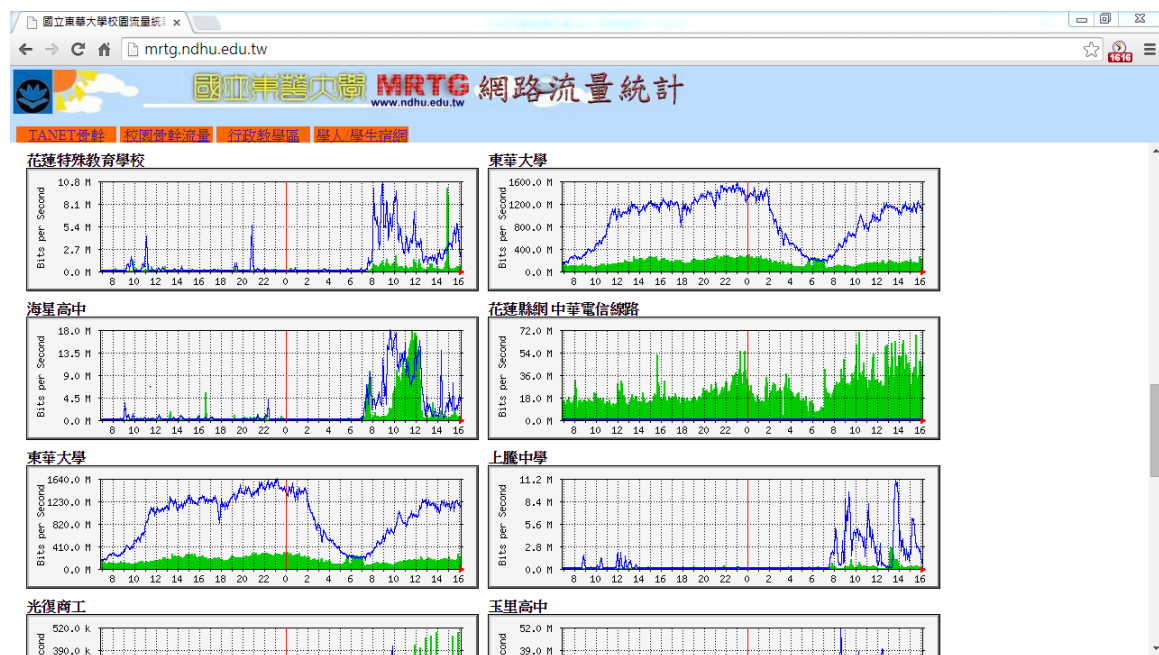
項目	Domain Name : Port	IP Address	機型	使用限制
DNS	dns.ndhu.edu.tw	163.28.160.11	Xeon 2.8G *2 1G DDR RAM 1U Server	開放花蓮區網中心 連線學校查詢
DNS	Dns2.ndhu.edu.tw	134.208.10.11	Xeon 2.8G *2 1G DDR RAM 1U Server	開放花蓮區網中心 連線學校查詢
Proxy Server	cache.ndhu.edu.tw: 3128	163.28.160.100	Xeon 2.8G *2 2G DDR RAM 5U Server	供東華大學及花蓮 區網中心所有使用 者使用。
Proxy Server	cache1.ndhu.edu.tw: 3128	163.28.160.110	Xeon 2.8G *2 2G DDR RAM 5U Server	供東華大學及花蓮 區網中心所有使用 者使用。
Proxy Server	cache2.ndhu.edu.tw :3128	163.28.160.120	Xeon 2.8G *2 1G DDR RAM 1U Server	供東華大學及花蓮 區網中心所有使用 者使用。
Proxy Server	cache3.ndhu.edu.tw: 3128	163.28.160.130	Xeon 2.8G *2 1G DDR RAM 1U Server	供東華大學及花蓮 區網中心所有使用 者使用。
BBS	bbs.ndhu.edu.tw :23	134.208.10.240	IBM PC Server	身份確認之使用者
SPAM Server	mg.ndhu.edu.tw	134.208.10.2	Xeon 3.0G *2 2G DDR RAM 2U Server	垃圾郵件防制軟 體，供東華大學所 有使用者使用及申 請使用之轄下連線 單位使用。
WWW	www.hdrc.edu.tw	163.28.160.14	Xeon 3.0G *2 4G DDR2 RAM 1U Server	無

(二) 工作內容

1. 網路管理

(A) 網路使用及流量統計分析

本中心已阻擋所有來自 TANet 骨幹網路之 P2P 流量，目前花蓮區網對 TANet 骨幹流量最大流入值約為 1624Mbps，平均流入值約為 940M，最大流出值約為 300Mbps，平均流出值約為 170Mbps；對 TWAREN 最大流入值約為 580Mbps，平均流入值約為 330M，最大流出值約為 130Mbps，平均流出值約為 53Mbps；對 HiNet 流量最大流入值約為 500Mbps，平均流入值約為 135M，最大流出值約為 200 Mbps，平均流出值約為 80M，流量統計相關資訊請參考 <http://mrtg.ndhu.edu.tw>。(詳如圖二)



圖二、MRTG 網路流量統計圖

(B) 資安事件檢舉處理機制

本中心接獲教育部轉知資安事件檢舉，先行封鎖被檢舉主機之 IP，讓出問題的主機不會繼續進行攻擊或發送廣告信，並於網站上公告被封鎖 IP，請被檢舉之使用者將主機進行修補或重灌，完成並確認後再行解除封鎖，並回報教育部資料司處理狀況，圖三為公告網頁。



NO	IP位址	區域	狀態	封鎖原因	封鎖日期
1257	134.208.5.163	行政教學區	關閉	後門攻擊custom: ET.TROJAN.ZeroAccess.Outbound.udp.traffic	2014-04-08
1260	134.208.21.144	行政教學區	關閉	後門攻擊	2014-04-15
1308	134.208.101.106	行政教學區	關閉	後門攻擊疑似對外進行殭屍網路行為	2014-09-15
1311	134.208.1.151	行政教學區	關閉	後門攻擊ips: NTP.Monlist.Command.DoS dropped	2014-09-24
1312	134.208.96.219	行政教學區	關閉	後門攻擊疑似對外進行殭屍網路行為	2014-09-24
1315	134.208.2.237	行政教學區	關閉	後門攻擊主機嘗試Host掃描攻擊	2014-11-11

圖三、資安事件檢舉處理公告網頁

除了被動處理外，本中心也採購網擎公司開發的 MailGates 垃圾郵件管理系統，讓本校使用者及連線學校自行進行垃圾郵件管理。這套系統功能包含：過濾名單、DoS 防禦、內容關鍵字過濾、垃圾信行為特徵過濾、自動學習過濾、政策管理過濾、條件群組設定和郵件記錄統計報表等，功能相當強大，誤判率相當低，如圖四所示為垃圾郵件管理系統個人化管理畫面。

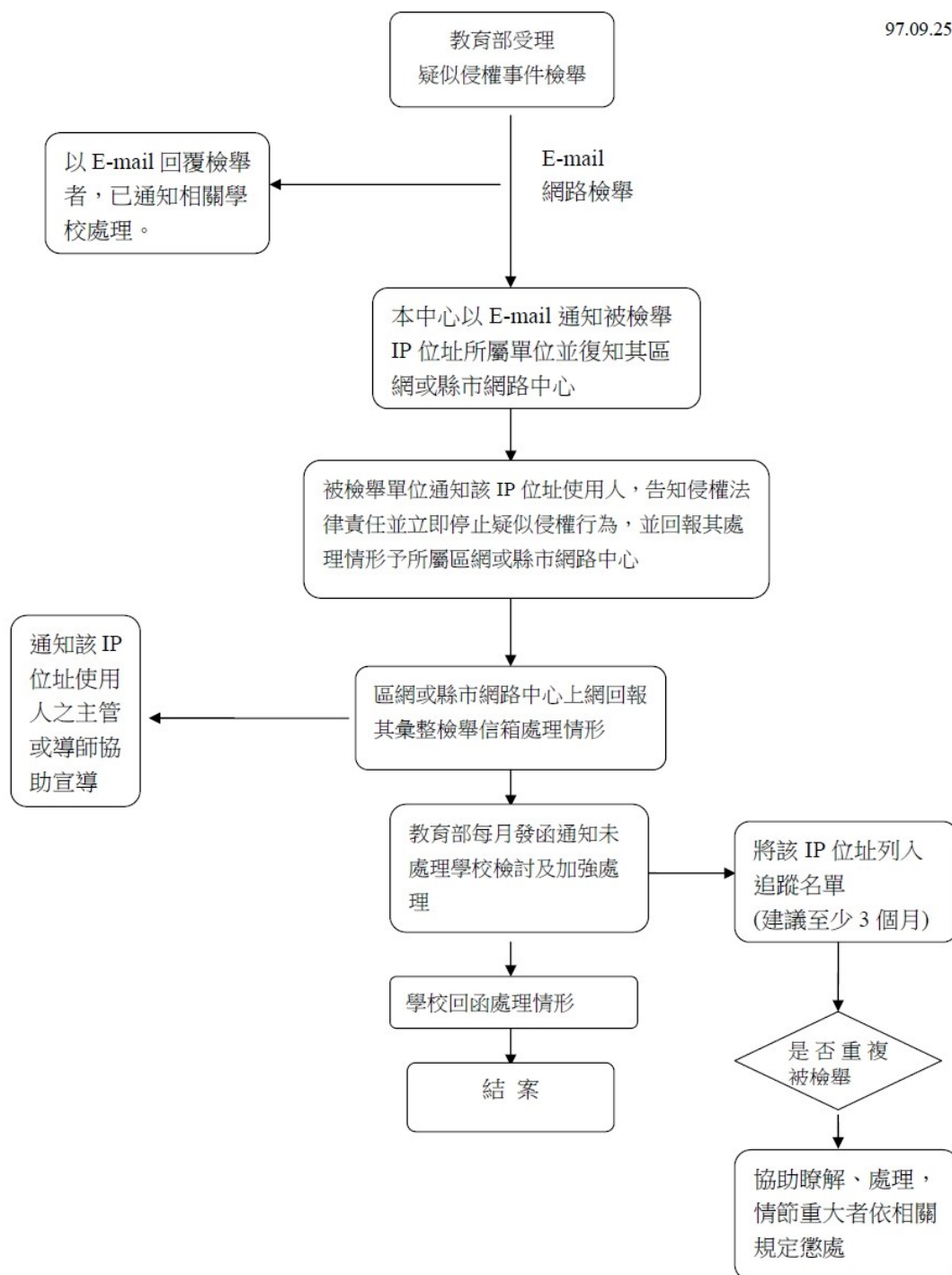


圖四、MailGates 垃圾郵件管理系統個人化管理畫面

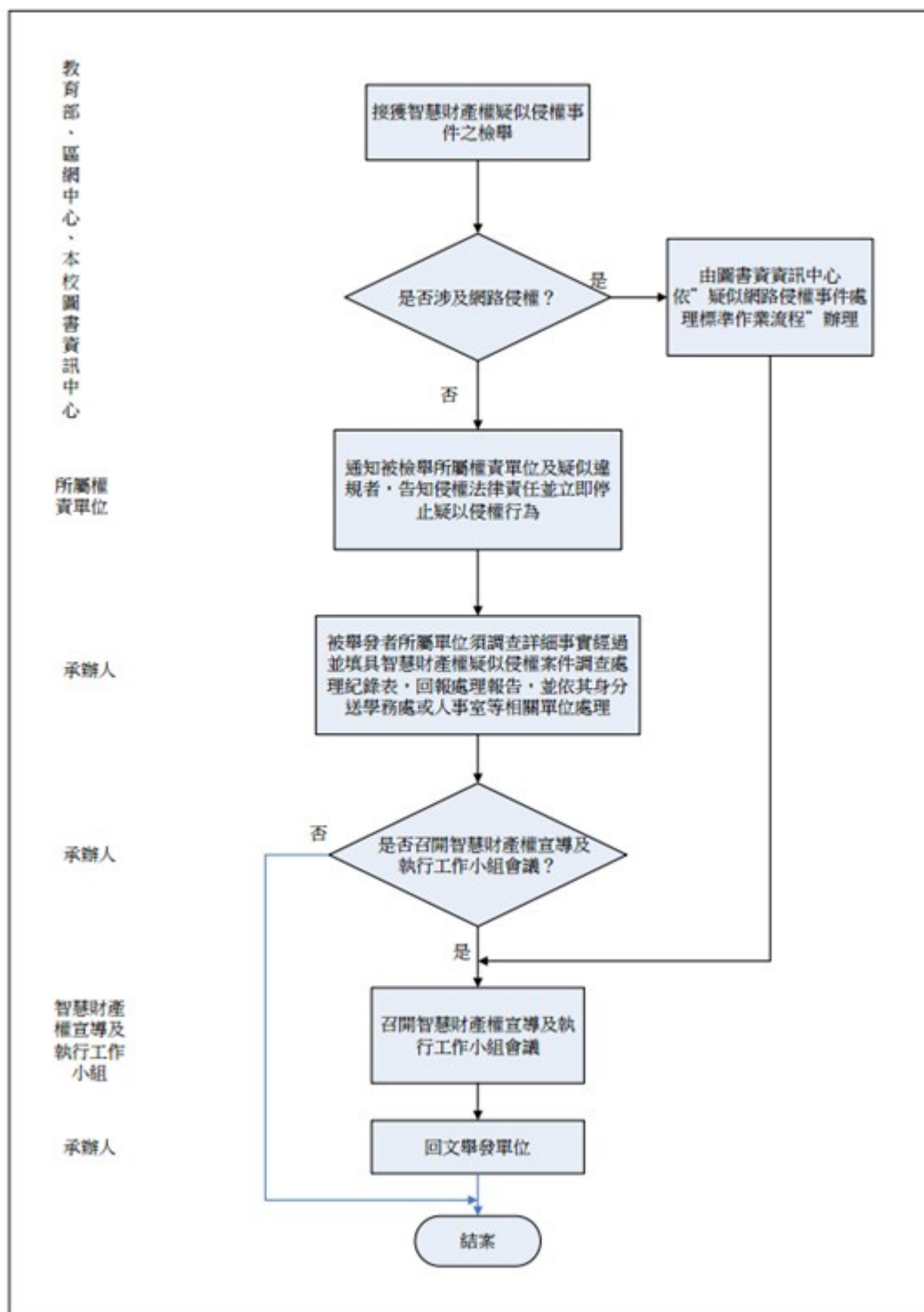
(C) 智財權檢舉案件處理

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的台灣學術網路智慧財產權疑似侵權處理程序，如圖五所示，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，第一時間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六所示。

惟自民國 99 年以來，本校因使用資安設備如入侵偵防設備、頻寬管理器等，阻擋來自 TANet 及 Hinet 的 P2P 流量，103 年至今侵權事件為 0。



圖五、台灣學術網路智慧財產權疑似侵權處理程序



圖六、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

為提高本區網中心連線單位網路管理委員會出席率，本年度規劃未來每年召開的兩次連線單位會議將於本校美崙校區舉辦，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。

由於花蓮縣幅員狹長，本區網中心在花蓮縣北區所舉辦的各式資安、個資或網路技術等研討會，中、南區的學校無法參與，地理因素也間接地造成資訊落差，為此，本區網中心規劃與花蓮縣偏遠學校合作，分別在花蓮縣中區或南區辦理資安研習，俾利偏遠地區的學校也有機會參加相關的資訊研討會。

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委員會外，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，如圖七所示，另外關於教育訓練我們也建置 e 化報名系統 http://labs.ndhu.edu.tw/seminar/seminarlist.php?page_serno=255，如圖八所示，此外，本中心也提供連線單位 proxy server、mail relay、dns、ftp 等各項網路服務。

4. 對區網連線單位提供 SIP Proxy 服務

本區網於 99 年 6 月 30 日完成建置 SIP Server 系統，目前 SIP Proxy server 安裝在兩部 Dell Server 上，IP 為 163.28.160.80 及 163.28.160.82，使用單位的前置碼為 936，管理單位的前置碼為 986。

目前提供連線單位網路語音交換服務計有 3 個單位，包括花蓮高中、花蓮女中及本校等，尚未連線的單位仍有 19 個，本區網將持續努力推廣中。



圖七、花蓮區網中心網站



圖八、花蓮區網中心-東華大學 TANet 教育訓練報名網頁

(三) 辦理資訊推廣活動

本中心於本年度預定辦理至少 6 場資訊推廣活動，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. 導入中央大學 Fdns 系統

階段一：本中心導入中央大學開發 TOP N 流量監測，可查詢異常連線行為與 IP 流量的統計，功能有：TOP N 流量、UDP

FLOODING、TOP C 流量、Port scan 統計等，如圖所示。

階段二：複製導入經驗，目前也正在建置專屬區網的 TOP N 監控系統。



IP 位址	輸入流量(MB)	輸出流量	輸入連接數	輸出連接數	輸入封包長度	輸出封包長度	輸入封包量	輸出封包量	紀錄時間
111.216.245.121	460	134	10	10	435	355	1057995	379572	11-12 04:40
134.208.33.216	215	638	61	18	388	357	555218	1784042	11-12 04:40
134.208.34.138	23	223	51	54	496	1112	46907	200877	11-12 04:40
134.208.38.7	6	105	697	1176	64	967	101184	109040	11-12 04:40
134.208.6.122	5	144	138	457	70	1273	75021	113599	11-12 04:40
134.208.33.216	116	242	42	14	477	247	244050	979764	11-12 04:30
134.208.34.138	16	174	41	48	406	1124	39498	154798	11-12 04:30
134.208.35.104	741	145	461	523	1185	312	626054	465551	11-12 04:30
134.208.34.138	10	155	26	31	370	1132	29060	137707	11-12 04:20
134.208.35.104	421	360	549	769	806	632	522918	570757	11-12 04:20
134.208.48.46	9	155	977	1273	64	990	148409	156966	11-12 04:20
134.208.3.181	2	171	15	23	46	1232	47024	139522	11-12 04:10
134.208.34.138	17	195	51	52	392	1121	44112	174644	11-12 04:10
134.208.35.104	48	210	503	479	307	888	159320	237332	11-12 04:10
134.208.48.46	9	160	925	1185	64	998	153512	160509	11-12 04:10
134.208.3.181	1	125	9	12	46	1237	32445	101581	11-12 04:00
134.208.34.138	18	173	50	55	456	1125	41434	154161	11-12 04:00
134.208.48.46	11	175	1049	1255	64	1001	173384	175320	11-12 04:00
134.208.35.251	6	104	781	918	64	1001	101295	104238	11-12 03:50
134.208.48.46	9	162	1097	1285	64	995	152890	162837	11-12 03:50

2. 規劃建置 TWAREN perfSONAR-based 網路效能監測系統

perfSONAR 可幫助網路管理者找出影響網路效能的原因並解決問題，即使跨越不同網域時，仍能輕易的解決點對點的網路效能問題，目前國網中心已經建立此套系統，也很樂意將技術資源分享，明年度將完成系統建置。

3. 建置本區網專屬的活動報名系統

考量使用校外不明的活動報名網站，會有個資外洩的風險，因此本區網在連線單位的建議下，規劃建置花蓮區網中心專屬的活動報名系統，以供連線單位使用。

4. 本校全面建置有 TANetRoaming 的 WiFi 熱點

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，以方便他校或 iTaiwan 的使用者得以使用本校的所有無線基地台。

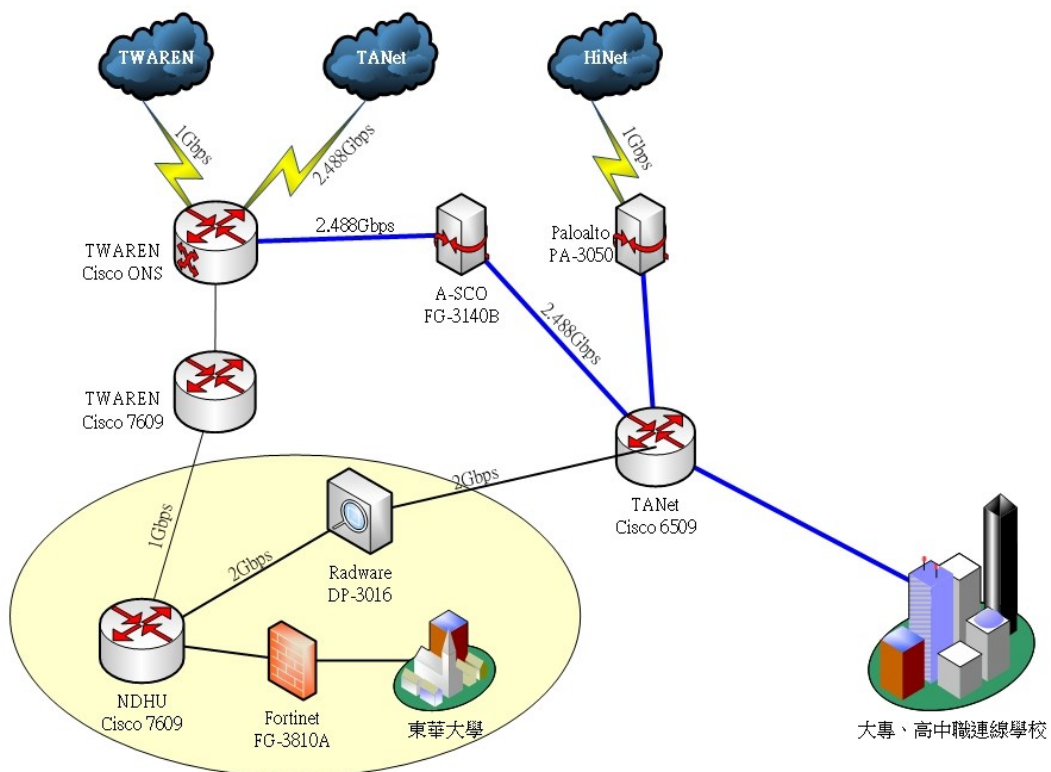
二、建構區網中心、連線單位及學校資通安全基本防護

(一) 現況說明(含網路架構圖)

1. 阻擋所有不正常的流量

本區網中心為防止連線單位內學生侵犯智財權，特別在 TAnet 及 Hinet 的入口分別安裝資安設備 Fortigate FG-3140B 及 Palo Alto PA-3050，將所有的 P2P 流量全部阻擋在外，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 Radware DP-3016 及防火牆 Fortinet FG-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十一所示。

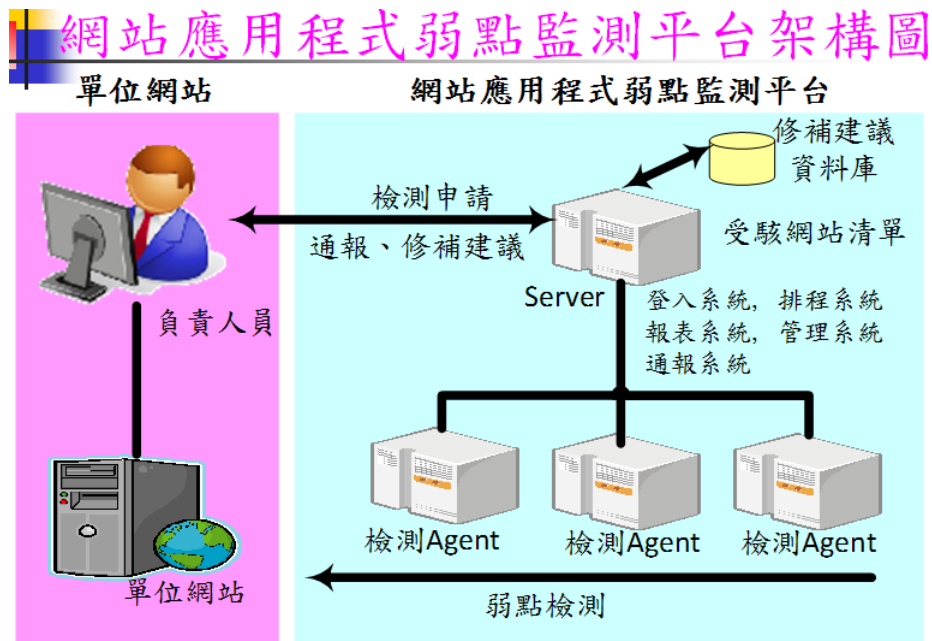
花蓮區網中心資安防護網路架構圖 (2014Q4)



圖十一、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技術，移轉之網頁弱點掃描監測機制與平台。並於 98 年 12 月建置完成，正式上線進行測試與調校。其架構如圖十二所示。本中心提供入口網頁供連線單位申請掃描服務，網址為 <http://ewavs.ndhu.edu.tw> 如圖十三所示。



圖十二、網站應用程式弱點監測平台架構圖



圖十三、網頁弱點掃描系統申請入

3. 防洩漏個資掃描平台

本平台提供 TANet 連線單位申請轄下網站個資掃描服務，針對網站開放區域即無經身份驗證可供任何人隨意存取之頁面進行特定類別個資掃描，並提供個資洩漏風險分析報告，作為網站個資揭露評估與相關避免個資洩漏處置措施的參考。本中心提供入口網頁供連線單位申請掃描服務，網址為 <http://ewavs2.ndhu.edu.tw/>，如圖十四所示。



圖十四、防洩漏個資掃描系統申請入口網頁

(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

將舉辦至少 6 場以上之資安技術、資訊相關教育訓練與活動，並提供轄下單位 Web Server 安全檢測服務及個資掃描服務。隨時提供相關資安諮詢服務：包含協助連線學校導入 ISMS、協助連線學校內稽等。

2. 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，本中心需二位專職人員，一位負責區網的網路維運，一位負責資安業務，其工作包含：

1. 負責花蓮區域網路的正常維運及故障排除。
2. 執行區網中心資訊安全管理制度(ISMS)業務。
3. 協助花蓮縣教育網路中心資訊安全網路實體防護業務。
4. 協助區網轄下各連線學校伺服器、網站安全掃描防護工作。
5. 協助區網轄下各連線學校處理資安通報應變及資安事件處理等相關問題。
6. 配合教育部TANet資訊安全技術服務團隊執行資安相關任務。
7. 執行教育部對本區網中心之交辦工作事項。

三、預期效益(KPI 指標)

1. 導入中央大學 FDNS 系統及網管應用系統
2. 建置 TWAREN perfSONAR-based 網路效能監測系統
3. 建置本區網專屬的活動報名系統
4. 提供連線單位資安防護達 17 所。
5. 預定至少辦理 6 場資訊與資安推廣活動
6. 到連線學校或偏遠地區至少辦理 2 場資安研習
7. 在花蓮市區召開本區網管理委員會至少 2 次。
8. 協助連線學校內稽作業至少 1 所。
9. 預定辦理資安推廣活動，連線學校相關人員參與數 200 人
10. 協助連線學校處理資安事件的通報與應變達 17 所

參、經費需求

詳列於附件、花蓮區域網路中心 104 年度基礎維運與資安人員計畫經費編列表。 本計畫經費合計：新台幣壹佰參拾玖萬整 (NT\$1,390,000)，向教育部申請全額補助 NT\$1,390,000 元。