

高屏澎 區域網路中心

「臺灣學術網路(TANet)區域網路中心 112 年度基礎維運與資安人員計畫」

民國 111 年 12 月

【 目 錄 】

壹、計畫基本項目	2
計畫期程	2
計畫執行單位	2
貳、計畫執行內容	2
一、區域網路中心基本維運現況說明	2
二、配合教育部資訊及科技教育司工作重點	2
(一)、網路管理	2
(二)、機房監控與管理	3
(三)、資訊服務	6
(四)、網管及連線管理	8
(五)、持續提供連線單位弱點掃瞄監測系統與網站應用程式弱掃系統	9
(六)、開發、建置並導入 TANet 不當資訊防護系統	11
(七)、承接 TANet 內容傳遞網路計畫(CDN)	13
三、112 年度區網中心工作重點及特色服務	16
(一)、應用特色服務	16
(二)、協助連線單位工作及應用服務推廣重點	17
(三)、辦理研討會及技術交流成果推廣會議	17
參、經費需求	17
一、人事費	17
二、業務費	18
三、設備費	18

壹、計畫基本項目

計畫期程

民國 112 年 1 月 1 日到 112 年 12 月 31 日

計畫執行單位

高屏澎區網中心
國立中山大學 圖書與資訊處 資訊安全組

貳、計畫執行內容

一、區域網路中心基本維運現況說明

- (一) 臺灣學術網路(TANet)高屏澎區域網路中心(也是台灣高品質學術研究網路的 GigaPOP)，提供區域內大高雄市、屏東縣、澎湖縣教育網路中心及大專院校與社會服務組織連接到學術網路的接取服務。
- (二) 中心除提供穩定與安全的網際網路連線外，並積極提供更好的網路服務品質和更佳的網路資源管理。對於大高雄市、屏東、澎湖區域內的各連線單位，可透過高屏澎區網中心首頁 (<https://web.kpprc.edu.tw>)取得各項相關的資訊與公告。除此之外，高屏澎區網中心亦提供異常流量分析及入侵服務偵測系統，有網路問題發生時，得以於最短時間內處理相關問題。

二、配合教育部資訊及科技教育司工作重點

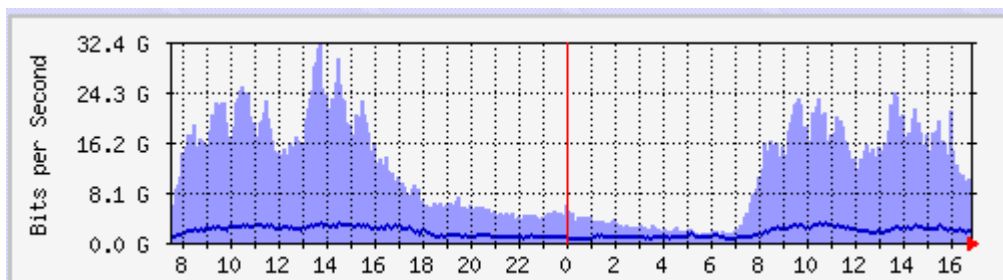
(一)、網路管理

1. 網路使用及流量統計分析

- (1) 高屏澎區網中心首頁 (<https://web.kpprc.edu.tw>)：提供本中心各項服務，並已取得 IPv6 Ready Logo。
- (2) 高屏澎區網中心 DNS (163.28.129.1 與 163.28.129.2)：提供給本區域內連線單位使用，IPv6 位址為 2001:288:8000::1:1、2001:288:8000::1:2。
- (3) 高屏澎區網 MRTG IPv4 流量統計，提供給本區域內連線單位網路流量狀況與資訊。

流量更新時間：2022 年 12 月 02 日星期五 16:48，來源

<https://192.83.166.83/mrtg/D00/D14/14-kpprc/kpprc-rc-core-ipv4.html>

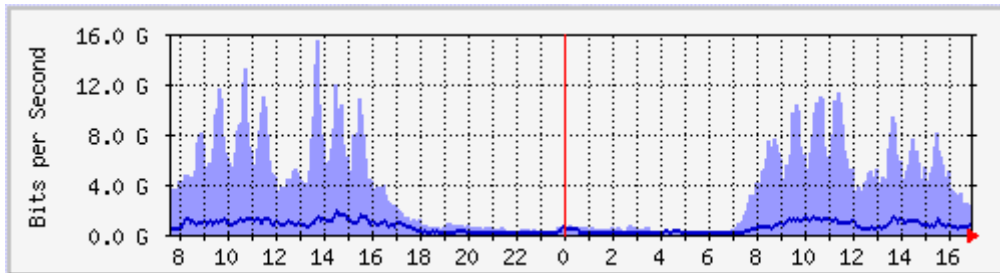


最大 In 32.2 Gb/秒 (7.5%) 11.3 Gb/秒 (2.6%) 9.3 Gb/秒 (2.2%)
最大 Out 3140.3 Mb/秒 (0.7%) 1650.5 Mb/秒 (0.4%) 1743.8 Mb/秒 (0.4%)

(4) 高屏澎區網 MRTG IPv6 流量統計

流量更新時間：2022 年 12 月 02 日星期四 16:59，來源

<https://192.83.166.83/mrtg/D00/D14/14-kpprc/kpprc-rc-core-ipv6.html>

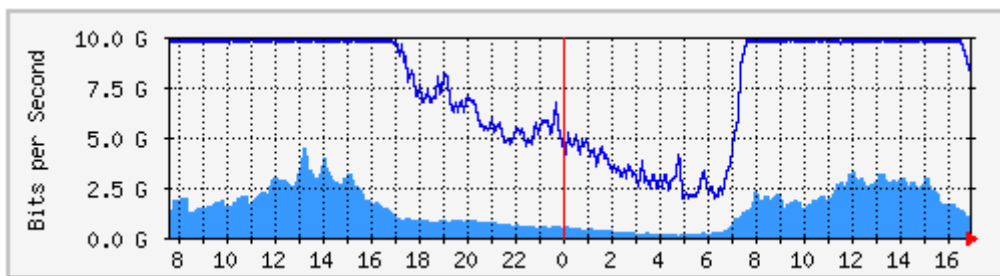


最大 In 15.4 Gb/秒 (3.6%) 3590.9 Mb/秒 (0.8%) 2212.3 Mb/秒 (0.5%)
最大 Out 1819.4 Mb/秒 (0.4%) 556.0 Mb/秒 (0.1%) 636.7 Mb/秒 (0.1%)

(5) 高屏澎區網 GGC-1 (Google Global Cache)：提供給連線單位更好的 Google 相關服務，並有效提升頻寬使用效率。

流量更新時間：2022 年 12 月 02 日星期五 17:17，來源

http://mrtg.kpprc.edu.tw/mrtg/192.192.60.117_111.html

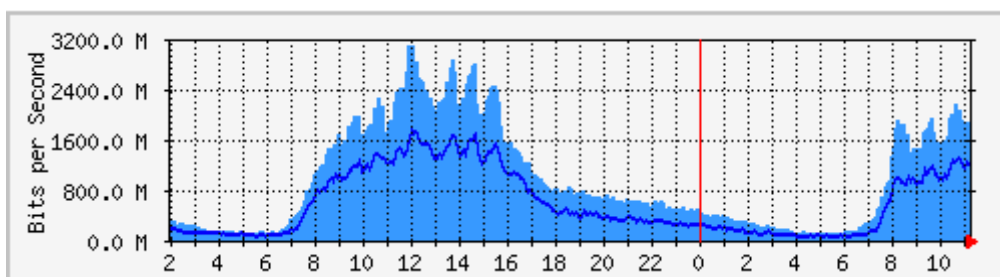


最大 In 4465.1 Mb/s (44.7%) 1448.7 Mb/s (14.5%) 1074.9 Mb/s (10.7%)
最大 Out 9884.7 Mb/s (98.8%) 7603.7 Mb/s (76.0%) 8687.4Mb/s (86.9%)

(6) 高屏澎區網 GGC-2 (Google Global Cache)：提供給連線單位更好的 Google 相關服務，並有效提升頻寬使用效率。

流量更新時間：2022 年 12 月 02 日星期五 17:20，來源

http://mrtg.kpprc.edu.tw/mrtg/192.192.60.117_116.html



最大 In 3102.0 Mb/s (31.0%) 953.3Mb/s (9.5%) 986.1 Mb/s (18.7%)
最大 Out 1732.3 Mb/s (98.8%) 577.2 Mb/s (76.0%) 1141.1Mb/s (11.4%)

(二)、機房監控與管理

1. 空間狀況：

高屏澎區網中心將 ASR 9010 放置在中山大學機房機櫃中，依照 ISO27001 之實體與環境安

全之建置及強化機房實體安全與系統網路管理，讓機房環境可隨時監測及控制。

2. 電力狀況：

- (1) ASR9010 設備的電力平常由台電的市電供給，同時連接到地下二樓電器室 UPS，若有斷電情形則由 UPS 提供電力，且校方發電機值班人員會立即到達，以確定發電機順利啟動，而達到不間斷之電力供應（如圖一所示）。



圖一：電器室 UPS 設備

- (2) 為避免 TWAREN 網路設備運作時的電力中斷，本校圖書與資訊處已完成主機房電力雙迴路及雙電力備援之建置，藉此維持網路連線之穩定。

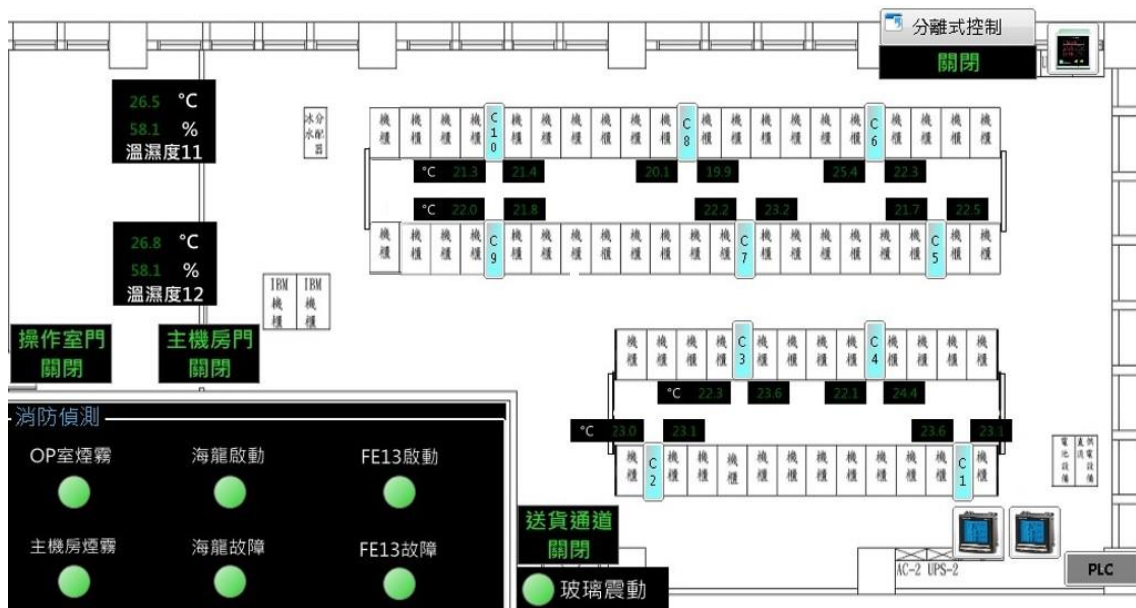
3. 空調現況：

- (1) 機房建置機櫃式空調（如圖二所示），並將區網核心路由器 ASR 9010 放置在機櫃式空調環境中，以提供更穩定的空調環境。



圖二：本機房所使用機櫃式空調

- (2) 機房之空調狀況，除了上班時專職維運人員的監控外，非上班時間亦可透過環控系統的 WEB 監控頁面，隨時隨地監控機房狀態(如圖三所示)。



圖三：本機房之環控系統

4. 消防與安全管制：

- (1) 機房規劃有消防警示系統及自動滅火系統、氣體滅火控制器（含溫度監測之告警系統）（如圖四所示），且當有異常事件發生時，環控系統會自動發送簡訊給管理者。



圖四：本機房的消防警示系統

- (2) 機房出入口有門禁及監視系統(如圖五所示)，可 24 小時監控人員與設備的進出。



圖五：本機房之監視器

5. 其他：

- (1) 人員進出機房皆應於「機房進出登記簿」登記。
- (2) 設備進出機房需填寫「設備進出紀錄表」。
- (3) 持續受理高屏澎區網的大專院校介接新世代骨幹網路連線申請(升速)，於管理會中審查。

6. 本區網中心至 111 年度止，共完成 29 個連線單位的 IPv6 路由設定，其中，導入比率 97.14%，包括 3 個縣市網路中心及 26 個連線單位，分項條列如下：

- (1) 縣市網路中心：高雄市網、屏東縣網、澎湖縣網。
- (2) 連線單位：高雄醫學大學、實踐大學高雄校區、屏東大學、海軍官校、中山大學、高雄師範大學、高雄大學、屏東科技大學、義守大學、輔英科技大學、正修科技大學、文藻外語大學、大仁科技大學、陸軍官校、中正預校、高雄榮民總醫院、空軍官校、高雄空大、航空技術學院、慈惠醫專、育英醫專、高雄餐旅大學、高雄科技大學、美和科技大學、高雄科技大學(旗津校區)及高苑科技大學計 26 所。

(三)、資訊服務

1. 教育單位弱點檢測平台 (<https://evs.ncku.edu.tw/>)：提供給高屏澎區網連線單位申請掃描該單位網站是否有漏洞問題。
2. 協助連線單位網路與資安等各項問題處理與諮詢服務，如協助連線單位排除 DDoS 攻擊等問題，協同 TACERT、國網中心及臺灣大學 (ASOC) 做流量清洗。
3. 提供 DNS 虛擬機範本服務 (Bind 9.10 以上版本)，並提供範本說明文件，連線單位可依範本修改無痛升級至最新版本，以防止 DNS 相關資安漏洞。
4. 提供「DNS 升級及資安健檢服務」，本中心主動連絡連線單位夥伴，協助升級老舊 DNS 版本，採線上服務表單，方便申請。迄今年共協助八所連線單位夥伴成功升級及設定：包含中

正國防幹部預備學校、輔英科技大學、育英護理專科學校、國立屏東大學、美和科技大學、國立澎湖科大、屏東縣網及高雄師範大學。

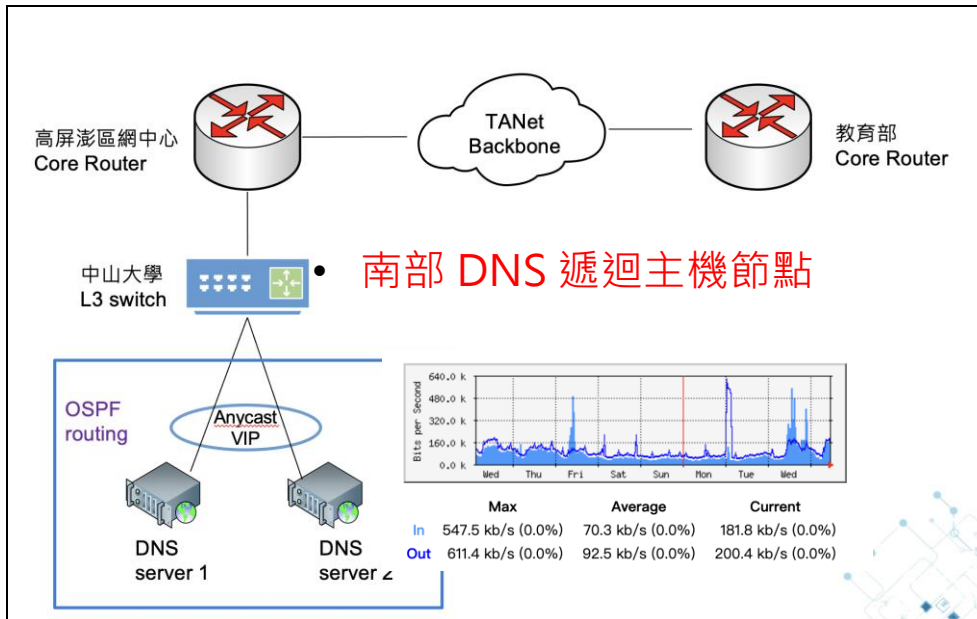
- 5. 111 年度獲教育部委託，進行 DNS 遞迴主機上線服務。

5-1. 台中以南學術網路將以中山遞迴主機為主進行查詢，降低北部負載，提升學術網路效率。

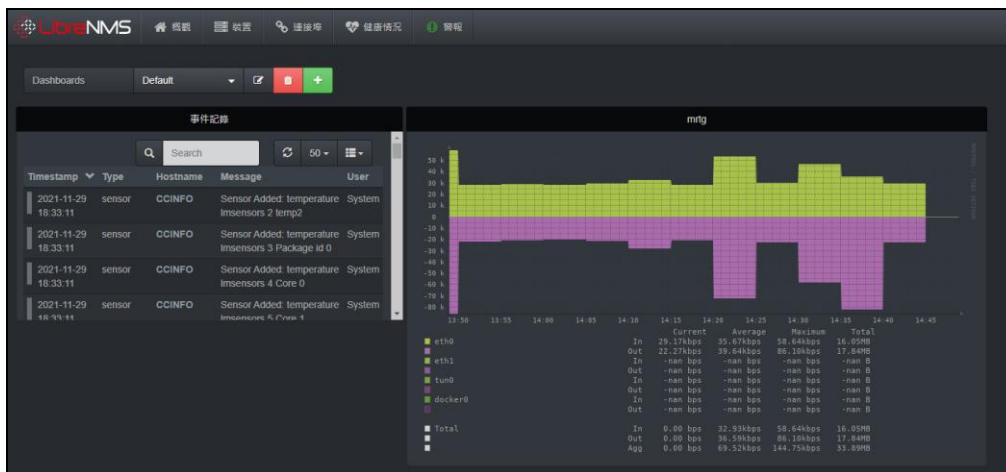
5-2. 本中心為求服務穩定另建置 HA 架構 SWITCH，以求服務穩定提供。

5-3. DNS 遞迴主機查詢服務，同時提供 HA 服務當北部據點無法查詢時，本中心據點可做為備援服務。

建置架構:



- 6. 本中心新推出容器化 LibreNms 網路裝置檢測平台供連線單位申請自行運用，採用容器化架構運行，加快轄下單位佈建，即時監測設備網路流量、硬體健康狀況，提升轄下單位縱深資安防禦與回報速度。



- 7. 於 98 年 7 月 20 日通過教育體系資訊安全管理規範 (ISMS) 之驗證，並取得證書；亦於今年 (111 年)11 月 22 日、23 日接受 SGS 稽核，受獲推薦即將取得國際版 ISO27001 資安認證，確保區網中心業務持續營運可以提供更安全及更穩定的區網網路服務。

- 8. 高屏澎區網中心網站弱點修正，加強網站資安，提供穩定查詢及公告服務。

修正重點

8-1. 將過去舊版套件產生之高中風險漏洞修正

8-2. 移除舊有套件遺留檔案降低入侵風險

8-3. 引進付費深度網站弱掃軟體 Acunetix 進行檢測，並修正風險值，降低網站遭受攻擊停擺服務。

弱點報告修正前後比對:

Alert Level	Count
High	1
Medium	3
Low	6
Informational	9

Alert Level	Count
High	0
Medium	0
Low	5
Informational	10

9. 協助高雄市、屏東縣及澎湖縣市網路中心骨幹頻寬升級

配合辦理臺灣學術網路(TANet)國內縣市教育骨幹頻寬升級案，協助設定高屏澎區網中心端網路及路由設定，提升網路連線頻寬。

9-1. 高雄市網：111 年 9 月 29 日完成頻寬電路建置及 Bundle-Ethernet 設定，頻寬由 40G 提升至 80G。

9-2. 屏東縣網：111 年 6 月 14 日完成頻寬電路建置及 Bundle-Ethernet 設定，頻寬由 20G 提升至 40G。

9-3. 澎湖縣網：111 年 8 月 31 日完成頻寬電路建置及 Bundle-Ethernet 設定，頻寬由 1G 提升至 2G。

10. 連線單位異常反應處理

111 年 9 月中 3 所連線單位反映與國網介接線路對 PING 有掉封包之問題其處理情形如下:

協助國網監測界接之設備 Router，發現於平日下午課程尖峰時段，有掉封包之情形，請國網中心進行效能分配調整，緩解此情形。

處理結果:

與國網中心討論後，請國網中心將該設備上連接之學校，規劃將使用流量較少之學校進行轉接至備援設備，將備援設備提升至 20G 頻寬，收攏更多掉封包之單位。

(四)、網管及連線管理

1. 服務偵測系統：採用 NAGIOS 系統為基礎，進行主機連線偵測，當所設定偵測的服務無法偵測時，將會把訊息回傳到個人 Google 行事曆。可設定偵測不同服務及 PORT，當該服務無法偵測時則發送告警，並將 Nagios 系統導入 HTTPS 服務，並整合 Nagios Check_ssl plugin，偵測 HTTPS 憑證到期日

系統網址：<https://mgmt.kpprc.edu.tw/nagios/>

2. Arcsight Logger 系統 (syslog 訊息監控)：將區網核心路由器 log message 導到此 log 管理系統，區網管理人員每日定期檢視是否有異常 log 出現並能立即處理。

系統網址：<https://logger.kpprc.edu.tw/platform-ui/>

3. Mrtg 流量監控連線單位界面流量狀態:提供連線單位夥伴查詢即時流量。

系統網址：<https://web.kpprc.edu.tw> (網路流量 MRTG 查詢)

4. Cacti 流量監控連線單位界面流量狀態:提供連線單位夥伴查詢即時流量。

系統網址：<https://web.kpprc.edu.tw> (網路流量 CACTI 查詢)

5. Cacti plugin weathermap :將網路流量以圖形化表現，不同顏色代表不同 Traffic Load，監控連線單位流量是否異常及過載。

系統網址：<https://web.kpprc.edu.tw> (網路流量 weathermap 查詢)

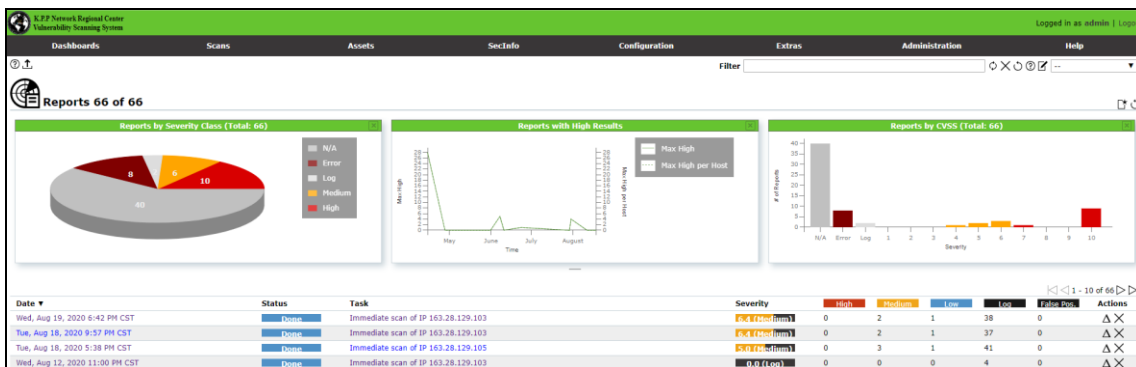
(五)、持續提供連線單位弱點掃描監測系統與網站應用程式弱掃系統

1. 說明：持續提供最新弱點定義庫與新版掃描引擎，呈現拓撲軌跡、風險弱點統計，協助連線單位掃描管控之伺服器目前開啟服務是否有弱點，以利連線單位網管人員針對弱點進行修正，防止駭客利用該弱點進行攻擊。

2. 功能簡介：系統提供弱點掃描後 LOG 檔匯出 PDF、XML 檔，排程掃描、批次掃描及自定義掃描。

3. 107 年 11 月開放申請以來共計 23 所單位申請，包含 23 所大專院校、1 所高中職、1 間醫院。

4. 風險報告及轉出：



風險報告轉出

Host scan start Mon Jun 8 00:06:27 2020 CST
 Host scan end Mon Jun 8 00:38:37 2020 CST

Service (Port)	Threat Level
80/tcp	High
3389/tcp	Medium
135/tcp	Medium
80/tcp	Medium

2.1.1 High 80/tcp

High (CVSS: 7.5)
 NVT: Apache Tomcat Multiple Vulnerabilities - Feb20 (Windows)

Product detection result
 cpe:/a:apache:tomcat:8.5.43
 Detected by Apache Tomcat Detection (Consolidation) (OID: 1.3.6.1.4.1.25623.1.0. ↪107652)

網站應用程式弱點掃描系統(109 年度新增)

1. 說明：本中心推出 Open Source 網站應用程式弱點掃描平台，採用 Ruby On Rails 架構提供跨平台執行，發佈 Windows 及 Linux 兩種版本，使用者可直接在本機直接執行，使程式開發者可以即時掃描修正弱點，提升網站安全。

2.系統畫面：

KPPRC Security Division, Web Application Vulnerability Scanning System.

Issues per scans, 'cause that's the way the cookie crumbles.

Notifications, about things you're involved in. Review your activity, to freshen your memory.

▼ Mark all read Scan http://140.117.13.128/WebSai/Wsai_Month (Default profile) started - Fri, 18 Sep 2020 05:58:22 +0000

3.弱點分析

Share Full edit Download report as: HTML JSON Marshal XML YAML AFR

The scan was aborted after 00:31:24.

Issues [23]

All [23] Fixed [0] Verified [0] Pending verification [0] False positives [0] Awaiting review [0]

Listing all logged issues.

TOGGLE BY SEVERITY

High	2
Medium	2
Low	2
Informational	17

NAVIGATE TO

SQL Injection	1
Blind SQL Injection (differential analysis)	1
Missing "Strict-Transport-Security" header	1
Common directory	1
Password field with auto-complete	1

URL Input

SQL Injection 1

Due to the requirement for dynamic content of today's web applications, many rely on a database backend to store data that will be called upon and processed by the web application (or other programs). Web applications retrieve data from the database by using Structured Query Language (SQL) queries.

To meet demands of many developers, database servers (such as MSSQL, MySQL, Oracle etc.) have additional built-in functionality that can allow extensive control of the database and interaction with the host operating system itself.

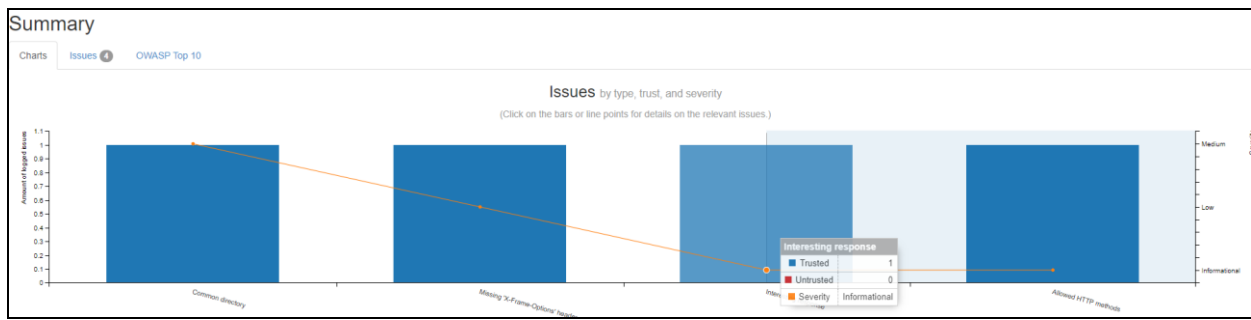
An SQL injection occurs when a value originating from the client's request is used within a SQL query without prior sanitisation. This could allow cyber-criminals to execute arbitrary SQL code and steal data or use the additional functionality of the database server to take control of more server components.

The successful exploitation of a SQL injection can be devastating to an organisation and is one of the most commonly exploited web application vulnerabilities.

This injection was detected as Arachni was able to cause the server to respond to the request with a database related error.

(CVE)

4.報表轉出

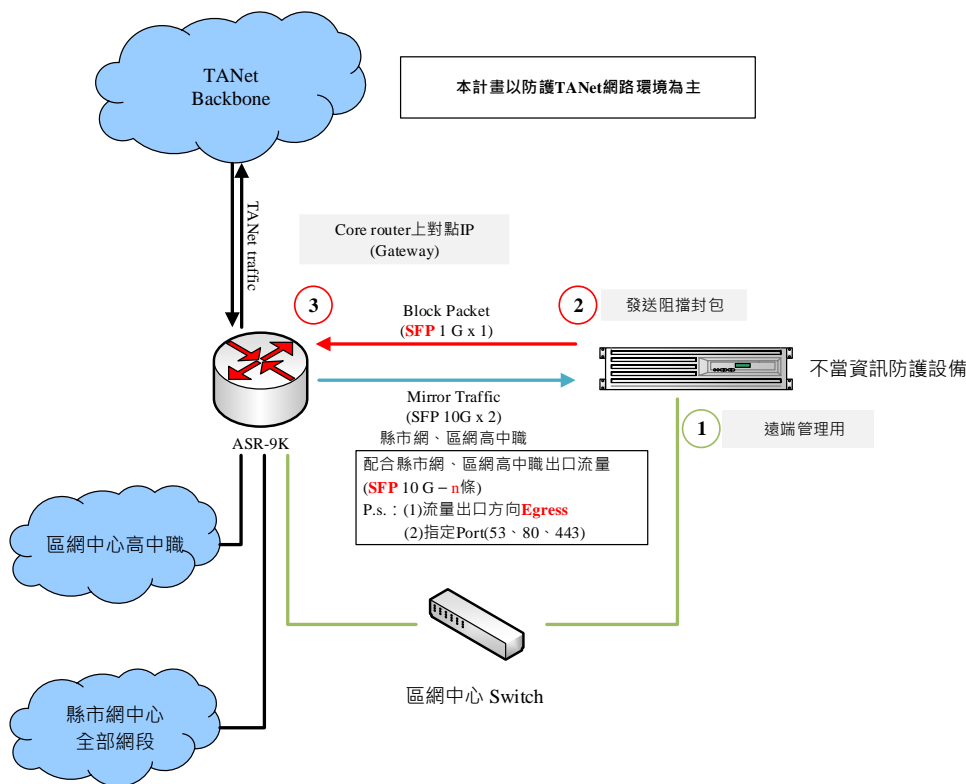


(六)、開發、建置並導入 TANet 不當資訊防護系統

1. 說明：109 年度高屏澎區網中心自行研發不當資訊防護系統技術，以防護 TANet 之高中職、國中小學及縣市網連線單位連線不當資訊網站(如暴力、色情、賭博等網站)，此系統主要特色如下：
 - 同時運用 Layer7 防護技術、DNS 防護技術及 IP 阻擋技術，將流量進行過濾，採用三重防護方式，提高防護效能。
 - 建置虛擬化伺服器 (VM Server)，進行系統環境測試，當系統遇突發狀況，透過 VM 即時測試與修正，避免因測試系統負荷量超載，造成設備故障問題產生。
 - 即時報表系統數據統計，提供系統過濾之每日瀏覽次數、每日阻擋次數及阻擋之不當網域及 IP 位置等統計資訊，另外依使用者 IP 的防護次數和不當網站的防護次數進行每月排名。
 - 模擬瀏覽測試程式開發，偵測需阻擋黑名單是否正確實阻擋，並檢視是否有誤擋情形發生，確保系統阻擋的正確性。
 - 資料庫管理，建立完整資料庫名單，完整囊括各大防護機制白名單及黑名單資料，並不定期去除無效網域位址名單。
 - 建置監控及資料派送系統，透過監控系統，監測各區網主機運作情況，並將資料庫黑白名單透過派送系統傳輸至各區網中心及縣市網中心，區網及縣市網之黑白名單資料庫亦可回傳至主系統中，進行資料更新。
 - 申訴檢舉平台建置，提供學術網路使用者於連線時，發現可建議系統阻擋的網站或使用者回饋已被阻擋意見之完整管道，由團隊進行問題排除並即時回報。
2. 高屏澎區網中心實際運作情形(目前已導入所屬全部國中小學及高中職連線單位)：
 - 縣市網：高雄市網、屏東縣網及澎湖縣網 (含所有國中小學)。
 - 高中職：左營高中、瑞祥高中及中正預校。
3. 各區網導入狀況：
 - 108 年度計畫已導入之區網中心：台北第一區網(臺灣大學)、台北第二區網(政治大學)、桃園區網(中央大學)、台南區網(成功大學)。
 - 109 年度計畫已建置(含已建置)：竹苗區網(交通大學)、雲嘉區網(中正大學)、花蓮區網(東華大學)。
 - 110 年度計畫已建置：台中區網(中興大學)、南投區網(暨南大學)。

- 111 年度計畫建置：宜蘭區網(宜蘭大學)(待建置)、台東區網(台東大學)(已建置)。
- 111 年度除宜蘭縣區網外，其餘縣市網皆已導入各區區網進行防護管理完成。

4. 系統佈署架構圖如下：

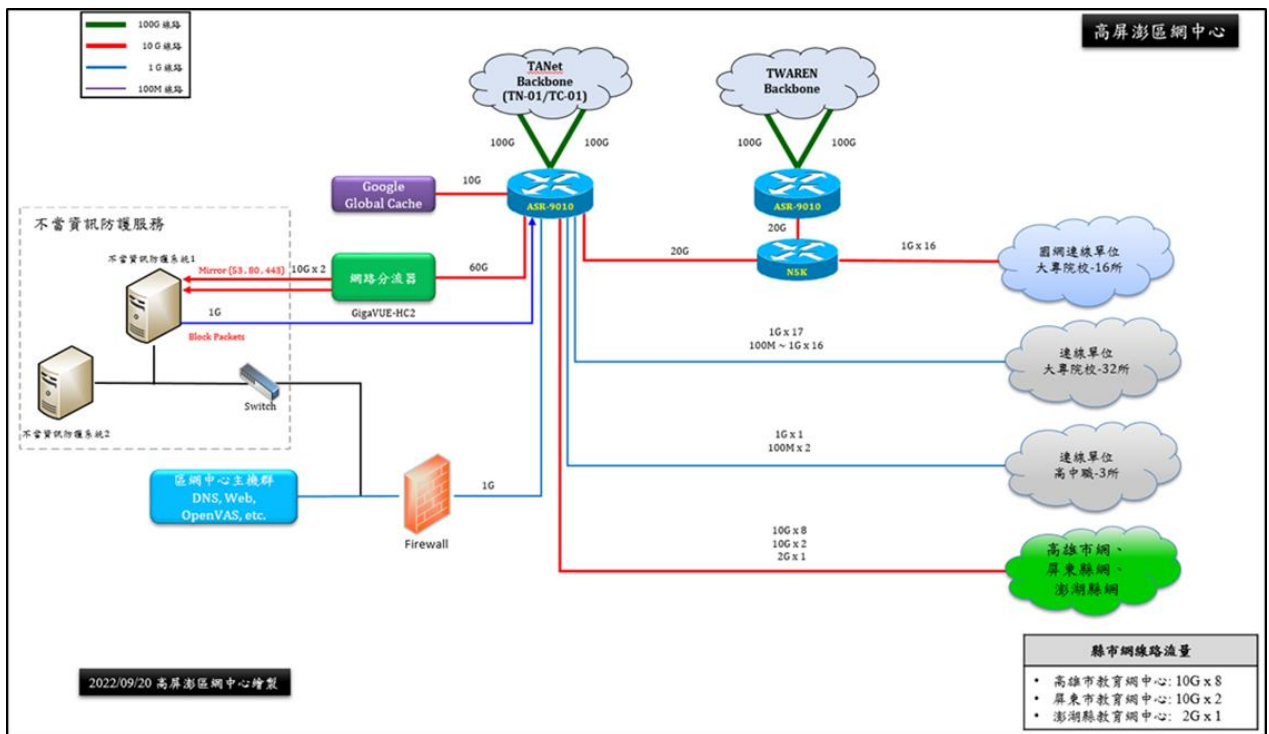


5. 導入現況如下：

	區網	縣市網中心	執行情況	設備種類
107 年度 (已完成導入)	高屏澎區網	高雄市	已導入	皆以 新採購設備 建置
		屏東縣	已導入	
		澎湖縣	已導入	
108 年度 (已完成導入)	臺北第一區網	臺北市	已導入	
		新北市	已導入	
	桃園區網	基隆市	已導入	
		桃園市	已導入	
		金門縣	已導入	
	臺南區網	臺南市	已導入	
109 年度 (已完成導入)	竹苗區網	新竹縣	已導入	
		新竹市	已導入	
		苗栗縣	已導入	
	雲嘉區網	雲林縣	已導入	
		嘉義縣	已導入	

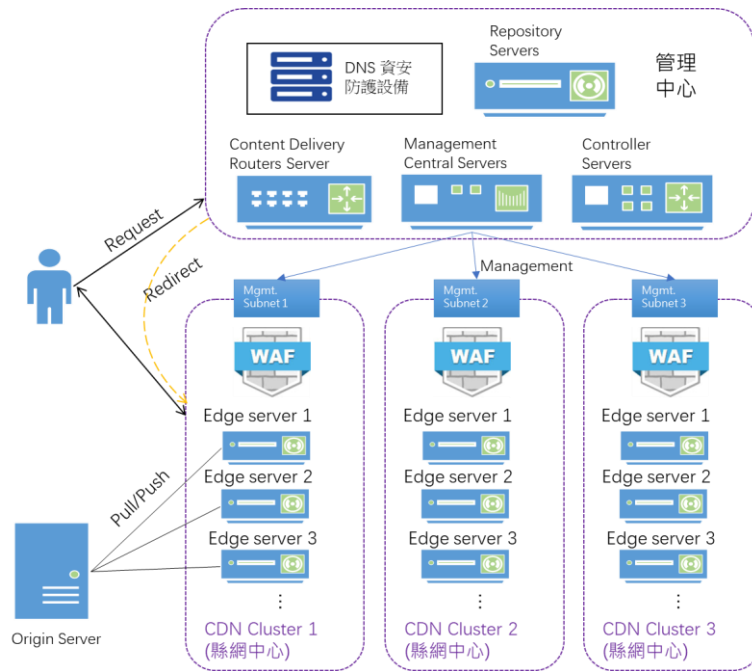
110 年度 (已完成導入)	嘉義市	嘉義市	已導入
	花蓮區網	花蓮縣	已導入
	南投區網	南投縣	已導入
	臺中區網	臺中市	已導入
		彰化縣	已導入
臺東區網	臺東縣	已導入	
111 年度 規劃導入	宜蘭區網	宜蘭縣	即將導入 (111 年 11 月)

6. 防護架構:



(七)、承接 TANet 內容傳遞網路計畫(CDN)

1. 計畫概述:目的在於建構適用於學術網路環境下的內容傳遞網路服務(簡稱:CDN)，用以改善臺灣學術網路的網路品質，藉此紓解目前頻寬壓力的問題。
2. 系統架構



3. 建置縣市網路中心分布表

項目別 縣市別	頻寬上限	學校數量 (所)	學生人數 (人)	計畫建置類別
臺北市	40 GB	1,006	337,313	六都
新北市	40 GB	1,493	471,977	六都
桃園市	40 GB	872	320,619	六都
臺中市	40 GB	1,130	409,744	六都
臺南市	40 GB	894	233,961	六都
高雄市	40 GB	1,092	333,884	範例、六都
屏東縣	20 GB	503	88,138	範例、非六都
新竹市	20 GB	227	81,362	非六都
南投縣	20 GB	370	58,462	非六都
嘉義縣	20 GB	306	44,434	非六都
澎湖縣	1 GB	78	9,377	離島

4. 管理中心分布表:

名稱	建置地點	地址
北區管理中心	教育部資訊及科技教育司	臺北市大安區和平東路二段 106 號 12 樓 (因機房空間問題, 目前建置於宜蘭區網中)

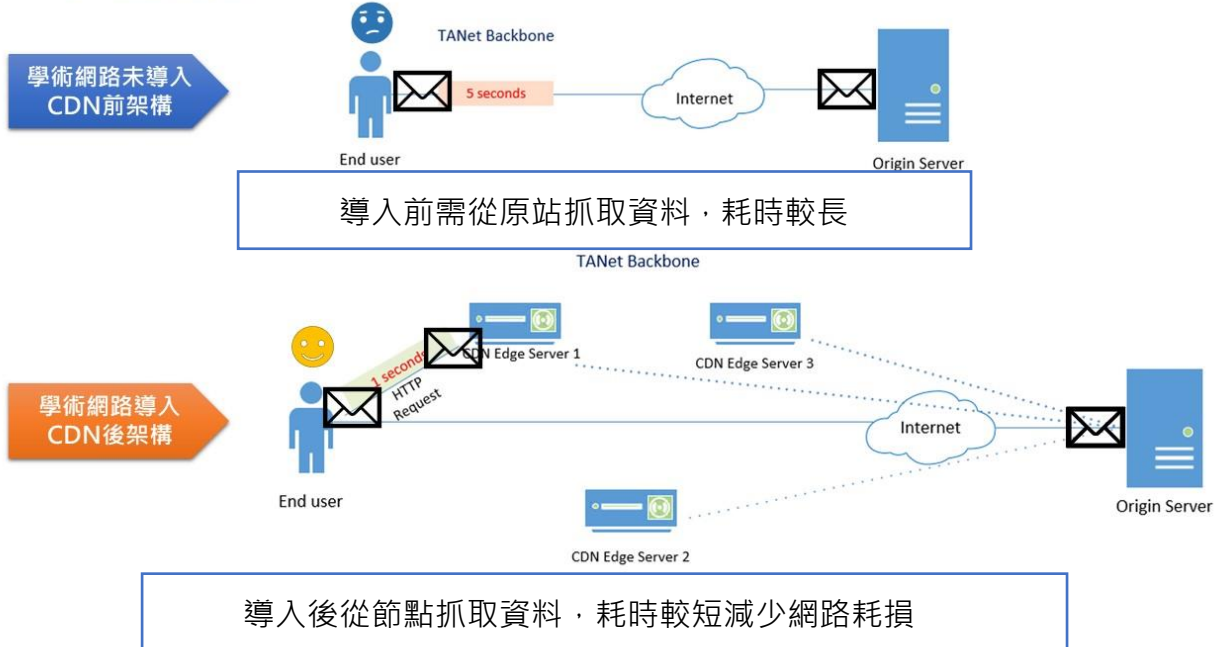
		心)
南區管理中心	國立中山大學圖書與資訊處	高雄市鼓山區蓮海路 70 號

5. 各階段建置表:

	完成建置及測試期限	建置範圍
第一階段： 部署前導開發環境	111 年 08 月 15 日前完成(已 完成)	管理中心：南區管理中心 高雄市網、屏東縣網
第二階段： 部署 CDN Edge 端點 及防護設備	111 年 09 月 30 日前完成(已 完成)	管理中心：北區管理中心 臺北市網、新北市網、桃園市網、 臺中市網、臺南市網、澎湖縣網
第三階段： 完成 CDN Edge 端點部署 及防護設備	112 年 01 月 15 日前完成	新竹市網、南投縣網、嘉義縣網

6. 導入前後比較

CDN導入前後之比較



三、112 年度區網中心工作重點及特色服務

112 年度工作重點將致力於提升區網中心資訊安全防護及維持網路維運穩定性，包含以下事項：

- 精進虛擬容器(container)弱點掃瞄系統及網路裝置監測服務系統。
- 持續精進網路異常流量分析服務、網站首頁異常置換偵測服務並調校偵測規則，同時提升監測網站數量。
- 協助連線單位有關 TANet 連線及資安相關問題排除。
- 持續推動區網中心與連線單位夥伴技術分享。
- 持續推動新增或更新容器化資安及網路監測系統。
- 不當資訊防護系統導入全國各區網中心:112 年度預計完成導入、宜蘭區網中心(宜蘭大學))及下轄之高中職與縣市網中心，為了提升不當資訊防護系統防護效能，並有效的管理及處理各區域使用者問題，青少年網路內容防護計畫開發之系統除持續優化防護技術，亦同時擴增其他系統服務，包含資料庫管理、全國數據報表系統、監控及資料派送等防護服務。
- 建置高屏澎區網中心黑名單阻擋分享平台，提供連線單位透過平台分享阻擋資訊，強化連線單位外對內網路防護能力與資安情資交換。
- 精進並優化 111 年度委員提供之建議。

(一)、應用特色服務

項目	KPI 指標
連線單位網頁置換監測服務	1. 導入連線單位網站首頁監測由 111 年 33 個網站提升至 60 個網站，成長率 90% 以上，以期多重監控服務，加強網站安全。
資安健檢服務	1.透過如 SHODAN 弱點搜尋引擎，尋找連線單位潛在資安弱點，並請連線單位做修正。 2.111 年共計 9 所，112 年提升至 15 所學校協助進行健檢服務，以期達 50% 以上成長率。
不當資訊防護系統導入	1. 112 年上半年完成宜蘭區網建置服務達成全台 100% 建置。 2. 針對六都區網頻寬提升，提供設備更換升級，112 年預計完成至少 3 都升級服務，完善防護系統(含備援機制)

<p>容器化系統精進推動</p>	<p>1.111 年累積共推出 3 種容器化網管、弱點監測、VPN 系統服務。 2.112 年預計推出至少 1 種容器化服務或更新改版，達成共計 4 套容器化系服務給連線單位分享使用。</p>
-------------------------	--

(二)、協助連線單位工作及應用服務推廣重點

項目	KPI 指標
<p>區網管理會及技術交流成果推廣會議</p>	<p>預計上半年及下半年各舉辦 1 場，共計 2 場。</p>
<p>應用服務推廣</p>	<ol style="list-style-type: none"> 1. 推廣網頁監測服務，廣邀連線單位申請加入監測。 2. 持續更新推廣主機弱點掃描 Container 服務及推出新款容器化服務。 3. VoIP 應用服務推廣 4. 建置黑名單分享平台廣邀連線單位加入分享 112 年預計至少導入 3 所學校。

(三)、辦理研討會及技術交流成果推廣會議

項目	KPI 指標
<p>辦理研討會</p>	<p>研討會：主題包括資訊安全、個人資料保護及網路技術相關等主題研討會，預計舉辦 4 場研討會以上。</p>

參、 經費需求

經費項目包括人事費、業務費、設備費，總計預算經費 **1,755,000** 元，其預算內容如附件一。

一、人事費

- (一) 網管人數 1 位，依據科技部補助專題研究計畫專任助理人員工作酬金參考表及參考工作年資編列（所具曾任年資經審定合於採計提敘者，得於本職高薪範圍內酌予提晉薪級，惟每滿一年最多提敘一級）。
- (二) 資安人數 1 位，依據科技部補助專題研究計畫專任助理人員工作酬金參考表及參考工作年資編列（所具曾任年資經審定合於採計提敘者，得於本職高薪範圍內酌予提晉薪級，惟每滿一年最多提敘一級）。
- (三) 網管人員、資安人員之勞健保費、離職儲金、補充保費。
- (四) 預算經費 **1,249,894** 元

二、業務費

包括講座鐘點費、膳費、差旅費、雜支、電信費、設備維護費、工讀費、週邊零件費、教育訓練費及工作費，預算經費 355,106 元。

三、設備費

包括網路設備、機房維護設備費、創新技術開發設備費，預算經費 150,000 元。

附件一

教育部補助計畫項目經費

申請單位：國立中山大學		計畫名稱：臺灣學術網路(TANet)區域網路中心 112 年度基礎維運與資安人員計畫			
計畫期限： 112 年 01 月 01 日至 112 年 12 月 31 日					
計畫經費總額： 1,755,000 元，向本部申請補助金額：1,755,000 元，自籌款：0 元					
經費項目		計畫經費明細			
		單價(元)	數量	總價(元)	說明
人事費	專任行政助理(資安)	39,400	13.5	531,900	資安專任行政助理 112 年 1 月~112 年 12 月薪資(含 1.5 個月年終獎金)。
	專任行政助理(資安)勞、健保	5,244	12	62,928	資安專任行政助理 112 年 1 月~112 年 12 月勞、健保費，依勞保投保金額級距 14 級距對照計算為\$5,244。
	專任行政助理(資安)勞工退休金	2,406	12	28,872	資安專任行政助理 112 年 1 月~112 年 12 月職儲金，依勞保投保金額 6%級距 14 級距對照計算為\$2,406。
	專任行政助理(資安)補充保費	1,247	1	1,247	資安專任行政助理年終工作金補充保費： $39,400 \times 1.5 \times 2.11\% = 1,247$ 元
	專任行政助理(網管)	39,400	13.5	531,900	網管專任行政助理 112 年 1 月~112 年 12 月薪資(含 1.5 個月年終獎金)。
	專任行政助理(網管)勞、健保	5,244	12	62,928	網管專任行政助理 112 年 1 月~112 年 12 月勞、健保費依勞保投保金額級距 10 級距對照計算為\$5,244。
	專任行政助理(網管)勞工退休金	2,406	12	28,872	網管專任行政助理 112 年 1 月~112 年 12 月離職儲金，依勞保投保金額 6%級距 10 級距對照表計算為\$2,406。
	專任行政助理(網管)補充保費	1,247	1	1,247	網管專任行政助理年終工作金補充保費： $39,400 \times 1.5 \times 2.11\% = 1,247$ 元
	小計			1,249,894	未依學經歷(職級)或期程聘用人員，致補助剩餘款不得流用。
業務費	講座鐘點費	2,000	9	18,000	依「教育部補助及委辦計畫經費編列基準表」之規定，外聘專家學者 2,000 元/Hr，3 小時/每場次。1 場合計 3 小時，共 3 場

教育部補助計畫項目經費

申請單位：國立中山大學		計畫名稱：臺灣學術網路(TANet)區域網路中心 112 年度基礎維運與資安人員計畫			
計畫期限： 112 年 01 月 01 日至 112 年 12 月 31 日					
計畫經費總額： 1,755,000 元，向本部申請補助金額：1,755,000 元，自籌款：0 元					
	工讀費	6,657	12	79,884	工讀生費用，工作為輔助技術人員業務相關行政及臨時交辦事項，其薪資為每月聘請 30 小時，時薪 176 預計月支出 5,280 計算+單位勞保負擔 908+補充健保 109+勞退 360，總計\$6,657*12 個月，採核實支付。
	膳費	120	120	14,400	膳費： 半天每人上限 120 元，每場次預計 40 人，共 3 場(早餐 50 元為限，午、晚餐以 80 元為原則、茶點一天只能一次，以 40 元為原則)。
	交通費	3,000	6	18,000	參加會議之交通費，單程以 3,000 元估算，預估 6 人次來回為 3,000*6 = 18,000 元(依國內出差旅報支要點辦理)。
	設備維護及租賃費	8,000	12	96,000	區網中心伺服器、VOIP、防火牆、資安防護等設備維護、租賃費、授權費用。預計每月 8,000*12 月=96,000 元
	電腦、通訊、周邊設備零件費	7,800	12	93,600	電腦及週邊設備零件、耗材等(單價未達一萬元之非消耗品)預計每月 7,800*12 月=93,600
	維護運作:辦公室電信、水費	300	12	3,600	網管警訊簡訊費、行動電話費、電話費用等每月 300*12 月=3,600
	專業證照教育訓練費	10,000	2	20,000	人員專業技能培養以提升區網維運及服務品質。教育訓練及證照考取等費用支出。 10,000 元/人，共 2 個人次。
	雜支	11,622	1	11,622	1. 凡前項費用未列之辦公事務費用屬之。如文具用品、紙張、資料夾、郵資等。 2. 單價未達 1 萬元或耐用年限未達 2 年
	小計			355,106	
設備費	網路設備費	40,000	2	80,000	因應學術網路頻寬增加，汰換區網中心伺服器網路集合使用之設備如 Switch、防火牆、高流量網路介面卡等。
	機房維護設備費	20,000	2	40,000	年度定期更換區網中心機房用品消耗，如:監視器設備、空調及消防設備等。
	創新技術開發設備費(伺服器)	30,000	1	30,000	區網中心特色服務用監控及討論會議用設備，直立伺服器及筆記型電腦。
	小計			150,000	

教育部補助計畫項目經費

申請單位：國立中山大學		計畫名稱：臺灣學術網路(TANet)區域網路中心 112 年度基礎維運與資安人員計畫		
計畫期限： 112 年 01 月 01 日至 112 年 12 月 31 日				
計畫經費總額： 1,755,000 元，向本部申請補助金額：1,755,000 元，自籌款：0 元				
合計			1,755,000	

附件一之一

教育部補(捐)助計畫項目經費表(非民間團體) 申請表 核定表

申請單位：國立中山大學		計畫名稱：臺灣學術網路(TANet)區域網路中心 112 年度基礎維運與資安人員計畫		
計畫期限： 112 年 01 月 01 日至 112 年 12 月 31 日				
計畫經費總額：1,755,000 元，向本部申請補(捐)助金額：1,755,000 元，自籌款：0 元				
擬向其他機關與民間團體申請補(捐)助： <input checked="" type="checkbox"/> 無 <input type="checkbox"/> 有 (請註明其他機關與民間團體申請補(捐)助經費之項目及金額) 教育部： 元，補(捐)助項目及金額： XXXX 部：.....元，補(捐)助項目及金額：				
補(捐)助項目	申請金額 (元)	核定計畫金額 (教育部填列) (元)	核定補助金額 (教育部填列) (元)	說明
人事費	1,249,894			1. 聘任專任行政助理(資安)1人，專任行政助理(網管)1人，本計畫人員共2人。 2. 所編費用含薪資、法定保險費用、勞退金、年終獎金及其補充保費。 3. 補(捐)助款不得編列加班費及應休未休特別工資。 4. 未依學經歷(職級)或期程聘用人員，致補(捐)助剩餘款不得流用。

附件一之一

申請表
核定表

教育部補(捐)助計畫項目經費表(非民間團體)

申請單位：國立中山大學		計畫名稱：臺灣學術網路(TANet)區域網路中心 112 年度基礎維運與資安人員計畫		
計畫期程：112 年 01 月 01 日至 112 年 12 月 31 日				
計畫經費總額：1,755,000 元，向本部申請補(捐)助金額：1,755,000 元，自籌款：0 元				
業務費	355,106			1. 講座鐘點費、工讀費、膳費、交通費等依講座鐘點費支給規定、二代健保規定、臨時人員薪資規範及國內出差旅費報支要點，訂有固定標準給付對象之費用。 2. 依國內出差旅費報支要點之相關費用。 3. 辦理業務所需、設備維護費、租賃費、電腦、通訊、周邊設備之介面、零件、維護運作費(辦公室電信費、水費、電費)、人員專業證照及教育訓練費等，依「教育部補助台灣學術網路區域網路中心管理作業要點」編列。 4. 雜支費用(凡前項費用未列之辦公事務費用屬之。如文具用品、紙張、資料夾、郵資等，單價未達1萬元或耐用年限未達2年)等依規定編列。
設備及投資	150,000			1. 建置區網中心創新服務使用之設備如伺服器、繪圖卡、高流量網路介面卡等。 2. 維護區網中心網路運作使用之設備，如：路由器、SWITCH。 3. 年度定期更換區網中心機房用品消耗，如：監視器設備、空調及消防設備等。
合計	1,755,000			
承辦單位	主(會)計單位	首長	教育部承辦人	教育部單位主管

附件一之一

申請表
核定表

教育部補(捐)助計畫項目經費表(非民間團體)

申請單位：國立中山大學	計畫名稱：臺灣學術網路(TANet)區域網路中心 112 年度基礎維運與資安人員計畫
計畫期程：112 年 01 月 01 日至 112 年 12 月 31 日	
計畫經費總額：1,755,000 元，向本部申請補(捐)助金額：1,755,000 元，自籌款：0 元	
補(捐)助方式： <input checked="" type="checkbox"/> 全額補(捐)助 <input type="checkbox"/> 部分補(捐)助 指定項目補(捐)助 <input type="checkbox"/> 是 <input checked="" type="checkbox"/> 否 【補(捐)助比率 %】 地方政府經費辦理方式： <input type="checkbox"/> 納入預算 <input type="checkbox"/> 代收代付 <input checked="" type="checkbox"/> 非屬地方政府	餘款繳回方式： <input type="checkbox"/> 繳回 <input checked="" type="checkbox"/> 依本部補(捐)助及委辦經費核撥結報作業要點辦理 彈性經費額度： <input checked="" type="checkbox"/> 無彈性經費 <input type="checkbox"/> 計畫金額 2%，計 _____ 元(上限為 2 萬 5,000 元)
備註： 一、本表適用政府機關(構)、公私立學校、特種基金及行政法人。 二、各計畫執行單位應事先擬訂經費支用項目，並於本表說明欄詳實敘明。 三、各執行單位經費動支應依中央政府各項經費支用規定、本部各計畫補(捐)助要點及本要點經費編列基準表規定辦理。 四、上述中央政府經費支用規定，得逕於「行政院主計總處網站-友善經費報支專區-內審規定」查詢參考。 五、非指定項目補(捐)助，說明欄位新增支用項目，得由執行單位循內部行政程序自行辦理。 六、同一計畫向本部及其他機關申請補(捐)助時，應於計畫項目經費申請表內，詳列向本部及其他機關申請補助之項目及金額，如有隱匿不實或造假情事，本部應撤銷該補(捐)助案件，並收回已撥付款項。 七、補(捐)助計畫除依本要點第 4 點規定之情形外，以不補(捐)助人事費、加班費、內部場地使用費及行政管理費為原則。 八、申請補(捐)助經費，其計畫執行涉及須依「政府機關政策文宣規劃執行注意事項」、預算法第 62 條之 1 及其執行原則等相關規定辦理者，應明確標示其為「廣告」，且揭示贊助機關(教育部)名稱，並不得以置入性行銷方式進行。	

※依公職人員利益衝突迴避法第 14 條第 2 項前段規定，公職人員或其關係人申請補助或交易行為前，應主動據實表明身分關係。又依同法第 18 條第 3 項規定，違者處新臺幣 5 萬元以上 50 萬元以下罰鍰，並得按次處罰。

※申請補助者如符須表明身分者，請至本部政風處網站(<https://pse.is/EYW3R>)下載「公職人員及關係人身分關係揭露表」填列，相關規定如有疑義，請洽本部各計畫主政單位或政風處。