

111年度竹苗區網第一次管理委員會

國立陽明交通大學 資訊技術服務中心

2022/5/27

目錄

1. 網站弱點檢測服務說明

1.1 HTTPS檢測現況說明

1.2 EVS平台網站弱點掃描

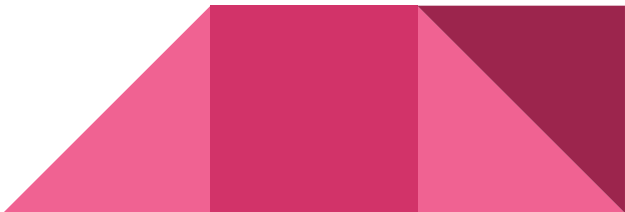
1.3 竹苗區網中心弱點掃描服務

1.4 資通系統安全檢測


2. 區網中心NetFlow設備更新事宜

3. TANet DNS 遞迴查詢服務

4. 臨時動議



1.1 HTTPS檢測現況說明


- 原依據110年6月29日臺灣學術網路技術小組第96次會議決議辦理之每季HTTPS檢測暫緩，待部內重新確認檢測工具及檢測方式後恢復辦理。
 - 有關HTTPS檢測現階段仍可使用TWNIC檢測工具檢測(<https://check.twnic.tw/>)，並自行修正網站HTTPS相關設定。
 - 目前區網中心有提供HTTPS檢測 Apache修正說明(https://www.hcrc.edu.tw/FAQ_index/all)。
- 

1.2 EVS平台網站弱點檢測

- 今年度截至5月竹苗區網連線學校使用EVS平台完成網站檢測次如如下表，各單位可多加利用EVS平台進行網站弱點掃描。
- 各連線學校若有帳號密碼遺失情形可直接聯繫本中心協助進行密碼重置。
- 現行各連線學校可申請檢測網站數為5個，若有其餘網站希望進行弱點檢測可申請區網中心Nessus弱點掃描服務。

年份	單位	狀態	單位數	網站數	檢測數	總執行時間	平均費時_分鐘	高風險網站數	中風險網站數	低風險網站數	無風險網站數	高風險頁數	中風險頁數	低風險頁數	信息提示頁數
2022	竹苗區域網路中心	執行失敗	1	3	9	1天17小時48分52秒	279	3	4	0	2	3	18	25	30
2022	竹苗區域網路中心	執行完成	6	15	22	1天0小時47分40秒	68	15	2	3	2	19	25	96	65

1.3 竹苗區網中心弱點掃描服務(1/3)

- 竹苗區網中心提供Nessus弱點掃描服務，各連線單位可置區網中心網站下載資訊服務申請表，經單位資訊主管簽核後掃描E-mail至區網中心承辦人信箱進行申請。
 - 區網中心審核後將由承辦人聯繫申請單位排定弱點掃描時間，弱點掃描完成後提供弱點掃描報告供申請學校參考。建議各單位於弱點修補完成後申請進行復掃。
 - 原則上各單位一年內申請掃描主機數量以10台為限，並於掃描完成一週後始得申請復掃。
- 

1.3 竹苗區網中心弱點掃描服務(2/3)

2. 對區/縣市教育網路中心

- 防火牆等網路安全
- DNS 系統的建置
- 網路系統的建置

資通安全防治

濫發廣告信(Spam Mail)、網路攻擊、不法網站處理

教育機構防洩漏個資掃描平台

3. 對區/縣市教育網路中心

- 建置竹苗區網防火
- mail relay (PC virus scanning)、web proxy server

教育單位弱點檢測平台

4. 竹苗區網弱點掃描服務

- 針對校園網站進行安全性掃描服務，提供資通系統管理者弱點掃描報告，各單位於弱點修補完成後可申請進行復掃。
 - 服務對象：竹苗區網中心下轄之資通系統管理人員。
 - 服務項目：對申請之資通系統執行安全性掃描服務。
 - 申請方式：請下載[資訊服務申請表](#)，並於貴單位資訊主管簽核後E-mail至竹苗區網承辦人信箱，區網中心審核後將由承辦人聯繫申請單位排定弱點掃描時間。
 - 相關業務，請與 h0631@nycu.edu.tw 連繫。

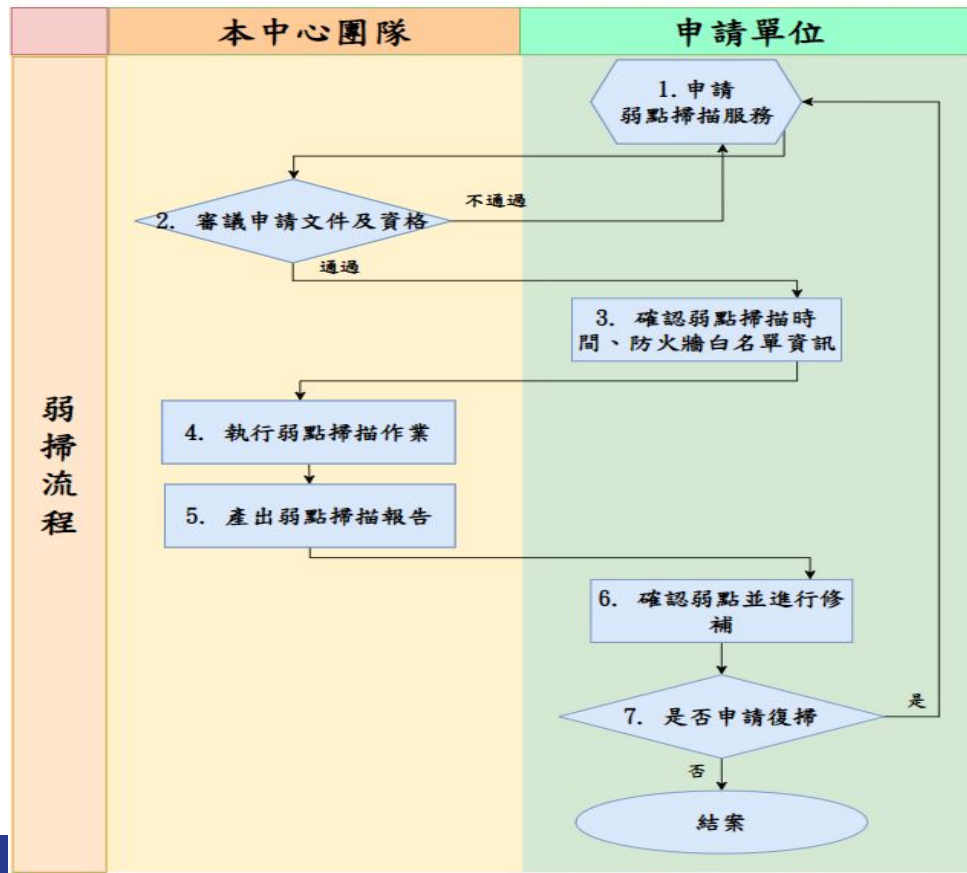
5. 竹苗區網防洩漏個資掃描平台相關服務

- 針對校園網站進行個資安全性掃描服務，提供網站管理者於發現網站有個資外洩之訊息報告時，網站管理者可及時修改網頁內容。
 - 服務對象：竹苗區網中心下轄之校園網站管理人員。
 - 服務項目：校園網站進行個資安全性掃描服務。
 - <http://epdp.hcrc.edu.tw/>
 - 相關業務，請與 h0631@nycu.edu.tw 連繫

6. 連線單位資安業務承辦人姓名、電話、E-Mail

1.3 竹苗區網中心弱點掃描服務(3/3)

- 竹苗區網中心弱點掃描服務申請及檢測流程如右圖
- 弱點掃描服務聯絡人：
 - 柯先生(h0631@nycu.edu.tw)
 - 廖先生(bo1206@nycu.edu.tw)

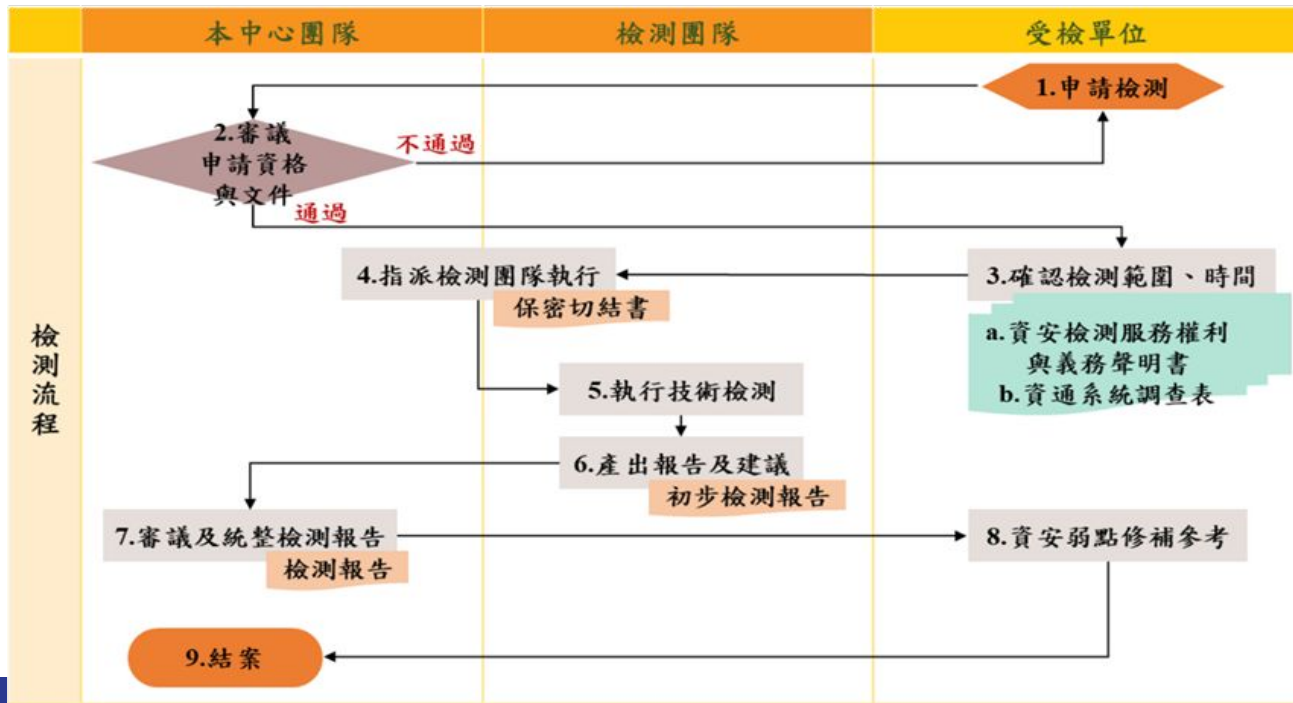


1.4 資通系統安全檢測服務(1/2)

- 竹苗區網中心辦理資通系統安全檢測服務，將由教育體系資安檢測技術服務中心(TACCST)培訓認可之技術檢測員及資通系統安全檢測學員實施。
- 即日起至111年6月10日(五)下午15:00止，受理線上登記，申請連結：<https://forms.gle/ghKNmchNA11uRYPK8>。
- 由本中心確認單位申請資訊後，以郵件方式回覆通知，詳細檢測日期及作業方式於申請通過後由本中心專人聯繫。
- 檢測服務聯絡人：
 - 竹苗區網中心－檢測作業：何小姐、呂小姐 hcrc@nycu.edu.tw

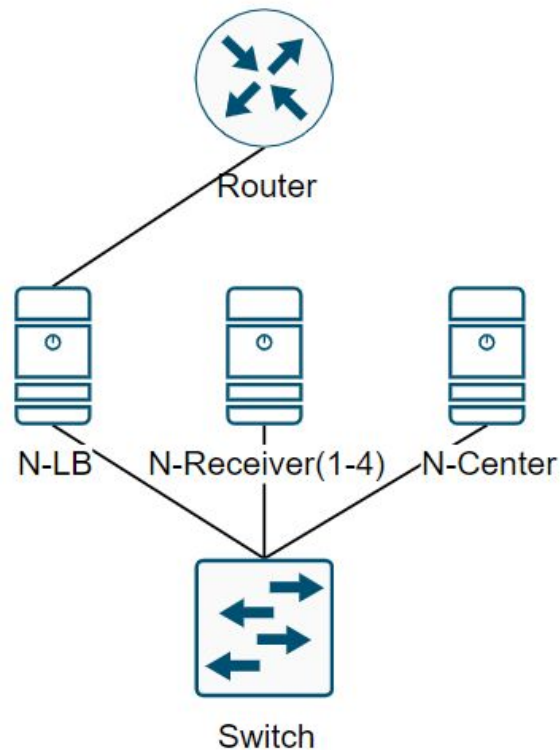
1.4 資通系統安全檢測服務(2/2)

- 竹苗區網中心辦理資通系統安全檢測服務，檢測流程如下：



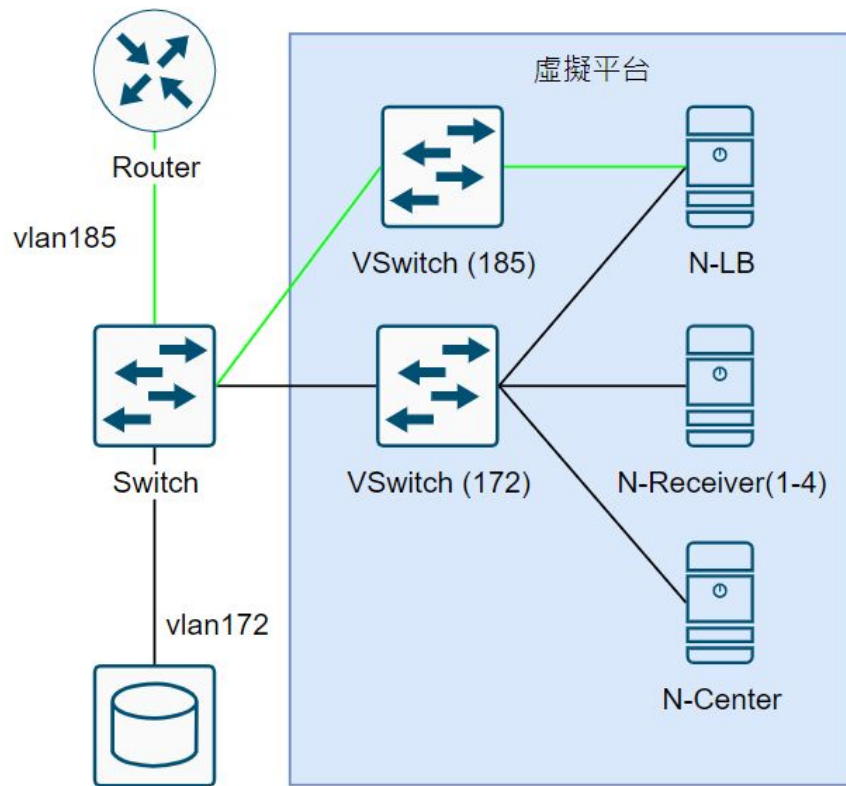
2. 區網中心NetFlow設備更新事宜(1/2)

- 現行N-Cloud架構由多台實體主機組成，由N-LB擔任對外服務IP，現行對外服務IP為140.113.0.185。
- 因現行設備無法支持升級新版本N-Cloud需求，故規劃將實體設備下架後回原廠進行硬體設備升級作業。



2. 區網中心NetFlow設備更新事宜(2/2)

- 完成N-Cloud設備升級前，將所有資料備份至虛擬平台上建置之臨時架構持續提供服務。
- 待新設備完成升級建置後將再次進行切換，因新版本N-Cloud無法相容舊版本資料，故臨時架構資料將留存3個月備查。



3. TANet DNS 遞迴查詢服務(1/3)

- 臺灣學術網路(TANet)網域遞迴查詢服務DNS主機IP位址資訊如下：
 - 1號機: 140.111.233.5(2001:288:0:233::5)
 - 2號機: 163.28.6.1(2001:288:1:1006:163:28:6:1)
 - 原提供臺灣學術網路 (TANet)網域查詢服務之遞迴主機 (IP為140.111.1.20、140.111.2.60、163.28.6.22), 將自111年6月1日起停止服務, 請各使用單位預為因應。
- 安全措施: 臺灣學術網路(TANet)DNS主機阻擋下列惡意網站網域名稱解析, 且相關紀錄將供本部分分析及研究使用。
 - 行政院國家資通安全會報技術服務中心「惡意中繼站網域名稱清單」。
 - 財團法人台灣網路資訊中心 (下稱TWNIC)RPZ機制阻擋之不法網站。
 - 內政部警政署(下稱警政署)「衍生性金融投資詐欺網址彙整表」。
 - 內政部警政署刑事警察局(下稱刑事局)「涉及詐欺案件之非法網站清單」。

3. TANet DNS 遞迴查詢服務(2/3)

- 未來將不再轉TWNIC、警政署、刑事局檢送惡意網站清單，改公布於TANet網路維運中心網站(下載資料需登入帳號，網址為<https://noc.tanet.edu.tw>)，如學校未使用臺灣學術網路(TANet)網域遞迴查詢服務，需設定校內DNS阻擋惡意網域解析，請自行至TANet網路維運中心網站下載。

The screenshot shows the website header for "臺灣學術網路 - 網路維運中心 TANet Taiwan Academic Network - Network Operate Center". The navigation bar includes "首頁", "公告", "流量", "網站", "工具", "下載", "維運", "通報", and "登出". The "下載" menu is open, showing options like "教學課程", "研討資訊", "影片(100G)", "Siraya 網管系統相關影片及講義", and "刑事局公告非法網站黑名單". A red box highlights the "刑事局公告非法網站黑名單" option. Below the menu, a table lists notices, with a red box highlighting the entry "[轉發]刑事局4月份涉及詐欺案件之非法網站清單下載".

1

2

3

3. TANet DNS 遞迴查詢服務(3/3)

- 因近期TANet NOC網站有大量惡意註冊行為故先行關閉註冊功能，各位老師若有需要申請TANet NOC網站帳號，可直接以公務信箱寄信至 moenoc@mail.moe.gov.tw，附上您要註冊的帳號名稱聯絡資訊即可。

4. 臨時動議

