臺中市 101 年度高中職以下各級學校資訊網管人員第 2 次研討會會議資料

《會議流程》

08:00~08:30 報到
08:30~10:00 教網中心工作報告
10:00~12:00 專題演講(一)
12:00~13:00 午餐
13:00~15:00 專題演講(二)
15:00~16:30 綜合座談

教網中心各組工作報告：

《校務系統組》

※101 年上學期資訊組長會議校務系統組報告※

I. SFS3 已支援自然人憑證登入及彈性的認證強度設定：
   - 功能開啟：至系統維護與管理(system)→憑證登入設定，啟用自然人憑證登入設定。
     - 系統須有 openssl 程式與支援 openssl_pkey_get_public 函式才能正常運作。
   - 認證強度區分：
     - (寬鬆) 校內外皆不限制。
     - (謹慎) 校內不限制, 校外須憑證。
     - (嚴格) 校內外皆須憑證。
     - (最嚴格) 僅能在校內以憑證登入。
   - 認證強度設定：模組權限管理(sfs_man2)→ 模組管理，針對模組設定不同的認證強度。
II. 學籍電子交換請協助校內人員全面改用 Open PGP 文件加解密輔助程式。(http://www.sfs.project.edu.tw/modules/news/article.php?storyid=127)
III. 使用 SFS3 圖書管理模組學校請建置教育部全國圖書系統介接機制。(http://www.sfs.project.edu.tw/modules/news/article.php?storyid=123)
IV. 因應 12 年國教免試入學，
   - 101 年 06 月 22 日已釋出社團活動(stud_club)模組。
   - 101 年 08 月 01 日已釋出服務學習(stud_service)模組。
   - 101 年 10 月 04 日已釋出 12 年國教 101 年中投區免試入學超額比序模擬作業(12basic_tcntc)模組。
   - 請安裝以上模組並會知相關處室人員。
V. 個資法施行細則已於 101 年 10 月 1 號施行，請系統管理員
   - 作業系統請更新至最新的版本，避免系統漏洞被駭。
     - 轉移 SFS3 至 Centos 6.3 平台講義參考：http://www.sfs.project.edu.tw/modules/mydownloads/visit.php?cid=2&lid=45。
   - 利用模組權限管理(sfs_man2)-權限列表全面檢視模組授權並宣導使用者勿將帳號密碼紀錄於便利貼或瀏覽器內。
   - 衡量學校情況，考慮將 SFS3 鎖在校園內，再透過其他機制自校外存取。或考慮採用新進已開發完成的憑證管理政策，進行個別模組的登入設定。
   - 為免除不必要的問題衍生，請學校將 SFS3 學務系統主機。
     - 設定防止搜尋引擎掃瞄抓取目錄資料(robots.txt、**User**-agent: * Disallow: /)。
     - 禁止 sfs3 送出目錄列表(httpd.conf --> AllowOverride 設為 All)。
VI. 部分國中學校因 2007-04-12 系統更新未成功，致本學年度新生匯入後，91 學年度學生基本資料被刪除
   - 請系統管理員利用學籍管理模組(stud_reg)檢查。
   - 有此情形學校可參閱 http://www.sfs.project.edu.tw/modules/newbb/

viewtopic.php?topic_id=3800&forum=3&post_id=10996#forumpost10996 解決。

VII. SFS3 學籍表、輔導紀錄表無法開啟錯誤處理：http://163.24.165.135/bookfee/sasdoc/guiderprt.pdf。

VIII. 支援臺中市政府一呼百應政策功能非官方模組

- 參考網址：http://www.sfs.project.edu.tw/modules/news/article.php?storyid=131。
- 行政用帳密儲存於模組變數。
- 導師若要使用可開啟級務管理(class_things)之模組變數(is_sms)使用。導師使用時，僅能發送予該班學生監護人，且帳密須自行登打。
- 問題與需求請逕洽該簡訊代發公司。

IX. 校內 IP 加入 IPv6 判斷，請自行於 config.php 加入校內 IPv6 網段判斷的變數 $HOME_IPV6。

《網路組》

一、網路連線記事

- 2012-05-01 所有學校 DNS IPv6 市網端反解設定完畢
- 2012-05-08 台中區網與 HINET 間 BGP peering 線路頻寬由 2Gb 擴增為 3Gb。同時網段 192.x.y.z、203.x.y.z、210.x.y.z 也直接開放和 hinet 交換路由。(MRTG 圖請參考台中區網 http://www.tcrc.edu.tw/flowmrtg.html)
- 2012-05-20 加入流量低限或斷線警報

○○○您好：以下為狀況通報 <<此為系統自動發信，請勿直接回覆此信>>

統計時間：2012-9-16 16:0:1

** 事件內容 **

斷線警報：無來自○○國小流量，持續 超過 30 分鐘。
流量低限警報：最近一小時來自○○國小平均流量低於 5byte/sec

斷線警報：根據前五分鐘流量，若發現無從學校送出之流量，或無送至學校之流量，則判斷為斷線，持續達一小時。前者主因多為電信業者或學校設備故障，請檢查貴校網路設備(例如重開機、檢查線路)，若無法解決請和電信業者或設備廠商連絡；後者極罕見則有可能是中心的路由器介面處於停止狀態 (shutdown)，或是電信業者線路問題，請和中心網路組連絡。
流量低限警報：最近一小時來自學校平均流量低於 5byte/sec，則判斷為低限。
補充說明：流量低限警報並非貴校處於斷線狀態，另一方面，若貴校在離峰(例如凌晨)時間，無人使用電腦及瀏覽貴校網頁(或連線)，則流量低限警報可視為貴校網路狀

況良好之特徵。
流量中限警報：最近一小時來自學校平均流量高於 1m byte/sec，會收到此警報

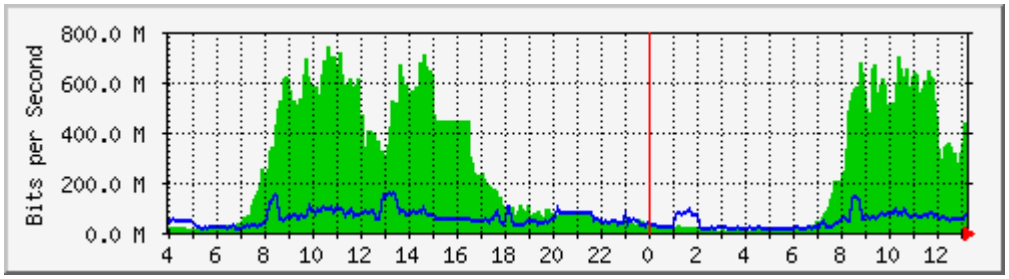
- 2012-07-13 新增連線單位：葳格高中、中科實中、台中特教學校
- 2012-08-03 WINDOWS 認證伺服器設定完畢
- 2012-10-15~19 101 年度行政院資通安全會報資安演練計畫

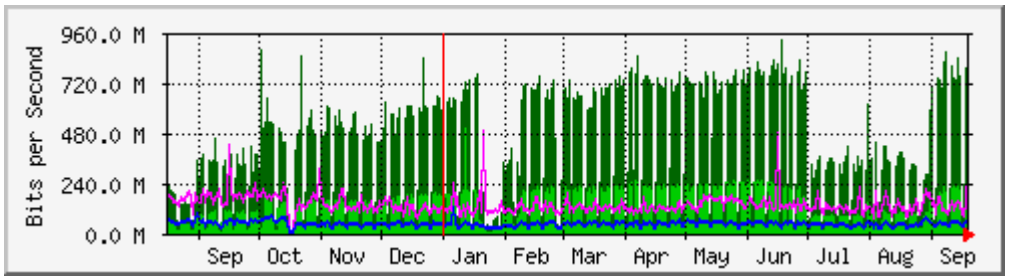
二、導入設定 DNSSEC

依據教育部 TANET 技術小組 85 次會議，考量 DNS 服務之穩定及安全性，導入 DNSSEC，目前已進行第一階段：區網中心建置完畢。第二階段將於縣市網路中心導入。台中市教育網路預計於 101 學年度導入 DNSSEC，屆時會提供文件供有興趣的學校設定。

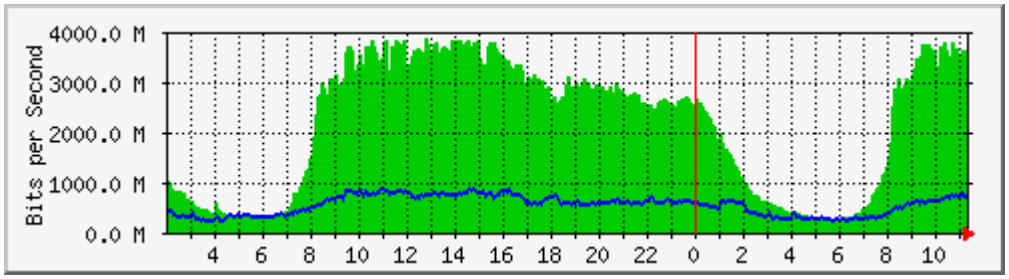
三、台中市網路頻寬使用已接近滿載，尖峰時刻有擁塞情況

http://mrtg.tc.edu.tw

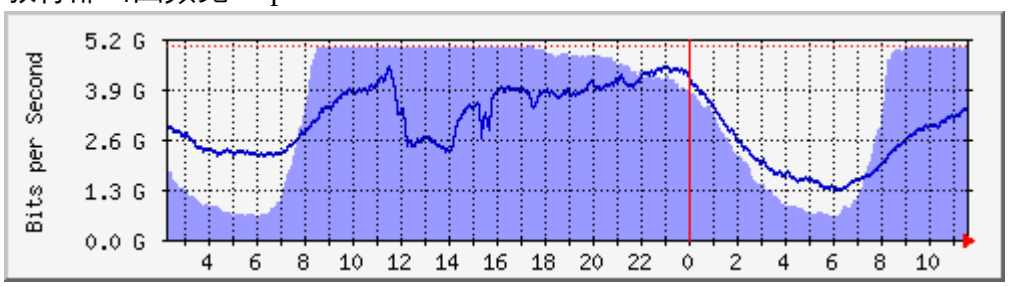




台中區網 http://www.tcrc.edu.tw/flowmrtg.html



教育部出國頻寬 http://192.83.166.25/tanet/internet/index.html



四、資安預警系統

service service@cert.tanet.edu.tw

資安聯絡人您好：

此為資安預警情報，請您協助確認資安預警事件(EWA)是否確實發生。

並登入資安通報平台後，於資安預警事件中完成通報作業，作業說明如下：

(如需相關佐證資料，登入通報平台後於事件附檔下載中依發佈編號即可取得。)

(1) 誤判：

經確認後設備相關記錄無符合項目，選擇「誤判」選項後，於「原因」處填寫說明。

(2) 確實事件：

經確認後確實發生資安事件，請先於自行通報中完成事件通報應變後，取得事件單編號後。選擇「確實事件」選項後，於右側填入自行通報事件單編號。

(3) 無法判斷：

經確認後，部份資料符合或設備相關記錄已不存在，選擇「無法判斷」選項後，於「原因」處填寫說明。

如果您對此事件單內容有疑問或有關於此事件之建議，歡迎與本單位連絡。

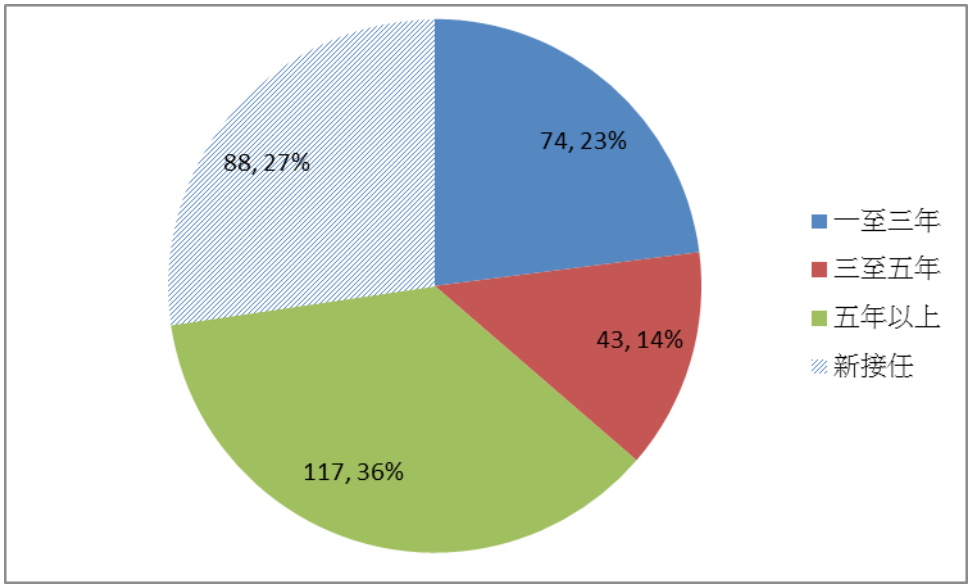
原發布編號	ASOC-EWA-201209-1300	原發布時間	2012-09-28 16:26:40
事件類型	對外攻擊	原發現時間	2012-09-28 16:21:06
事件主旨	通報:[○立◯◯◯◯學]163.x.y.z ips: Multiple.Vendor.ICMP.Remote.DoS detected		
事件描述	ASOC 發現貴單位(○立◯◯◯◯學)所屬 163.x.y.z 疑似對外進行 ips: Multiple.Vendor.ICMP.Remote.DoS detected 攻擊		
手法研判	惠請貴單位： 1.檢查防火牆紀錄：查看內部是否有開啟異常的連接埠。 2.利用工具程式(如:TCPview、procexp)於來源主機觀察，找出實際執行連線的程式，確認該程式是否為惡意程式。 3.若連線並非預期行為，則來源主機可能已遭植入惡意程式，建議利用木馬或後門清除程式掃瞄該主機，並手動檢測是否有惡意程式執行。 4.檢視及執行各系統之安全修補。		
建議措施	本攻擊相關資訊可於下列網址 http://www.iss.net/security_center/reference/vuln/ips: Multiple.Vendor.ICMP.Remote.DoS detected.htm 內查詢		
如果此事件需要進行通報，請 貴單位資安聯絡人登入資安通報應變平台進行通報應變作業			
如果您對此通告的內容有疑問或有關於此事件的建議，歡迎與我們連絡。			

收到此信請至 tacert 資安通報應變平台通報 https://info.cert.tanet.edu.tw/prog/index.php

五、未填報 101 學年度資安連絡人學校單位，請於會議中至前方來補填。

北區	立人國小	南區	明德女中	北屯區	葳格高中
西屯區	東大附中	豐原區	豐原高中	豐原區	豐原高商
后里區	啟明學校	潭子區	常春藤高中	潭子區	弘文高中
清水區	嘉陽高中	清水區	清水高中	大甲區	大甲高中
大甲區	大甲高工	大甲區	致用高中	沙鹿區	沙鹿高工
烏日區	明道中學	大里區	僑泰高中	大里區	立人高中
大里區	青年高中	霧峰區	明台高中	霧峰區	霧峰農工
太平區	慈明高中	東勢區	東勢高工	東勢區	玉山高中
東區	臺中家商	東區	臺中高農	南區	臺中高工
西區	臺中女中	北區	臺中二中	北區	臺中一中
西屯區	文華高中	南屯區	臺中特殊教育學校		
大雅區	中科實中	大里區	國立大里高中	西屯區	葳格中小學
大雅區	惠明學校	西屯區	東大附小	西屯區	臺中啟聰學校
中區	道禾實驗小學	北屯區	磊川華德福實驗學校		
南屯區	弘明實驗學校				

六、101 年度資訊組長資歷比例圖



七、IPv6 的首頁連通率及流量

各校首頁是否支援 IPv6 已列入今年度教育部統合視導評分項目，請各校務必使貴校首頁支援 IPv6。首頁有支援 IPv6 的學校(10/12 統計)

區域	支援 IPv6	校數	比率
沙鹿	11	13	84.6%
石岡	2	3	66.7%
南	4	7	57.1%
豐原	9	16	56.3%

大肚	4	8	50.0%
太平	9	21	42.9%
神岡	3	7	42.9%
潭子	4	11	36.4%
烏日	4	11	36.4%
后里	3	9	33.3%
外埔	2	6	33.3%
西	3	9	33.3%
龍井	3	10	30.0%
北屯	7	24	29.2%
霧峰	4	14	28.6%
大雅	3	11	27.3%
西屯	5	20	25.0%
新社	2	9	22.2%
大里	4	19	21.1%
大安	1	5	20.0%
東勢	3	15	20.0%
南屯	3	16	18.8%
大甲	3	16	18.8%
東	1	8	12.5%
梧棲	1	8	12.5%
和平	1	11	9.1%
中	0	1	0.0%
合計	**99**	**308**	**32.1%**

八、台中區網網路管理人員資料變更

轉知台中區網公告，今年度若各連線單位有網管人員異動者，請和台中區網連絡，目前資料請參考網址 http://www.tcrc.edu.tw/unit/people.php 電話 04-22840307#715 或網路電話 9311-0715

九、資安事件全校封鎖

全校封鎖 http://www.tc.edu.tw/net/netflow 已於今年 3/19 啟用

以下四種情況教網中心會將貴校所有網段予以限制與 Internet 連線權利（但仍可與教網連線）：

1、單一流量異常 IP 超過 30 日未解除。

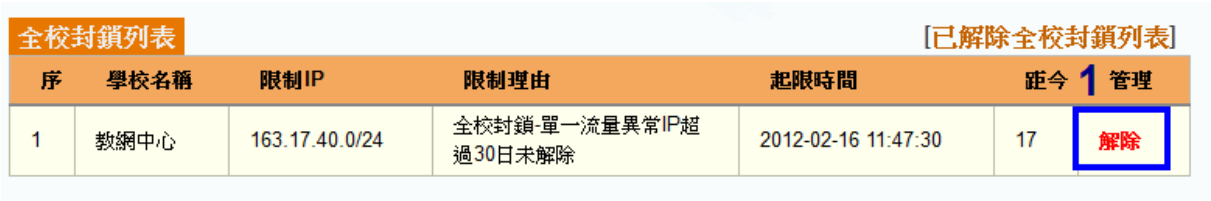
2、超過 5 個流量異常 IP 超過 7 日未解除。

3、一般資安事件超過 15 日未處理。

4、嚴重資安事件超過 1 日未處理(侵權、網頁置換、刑事案件等)。

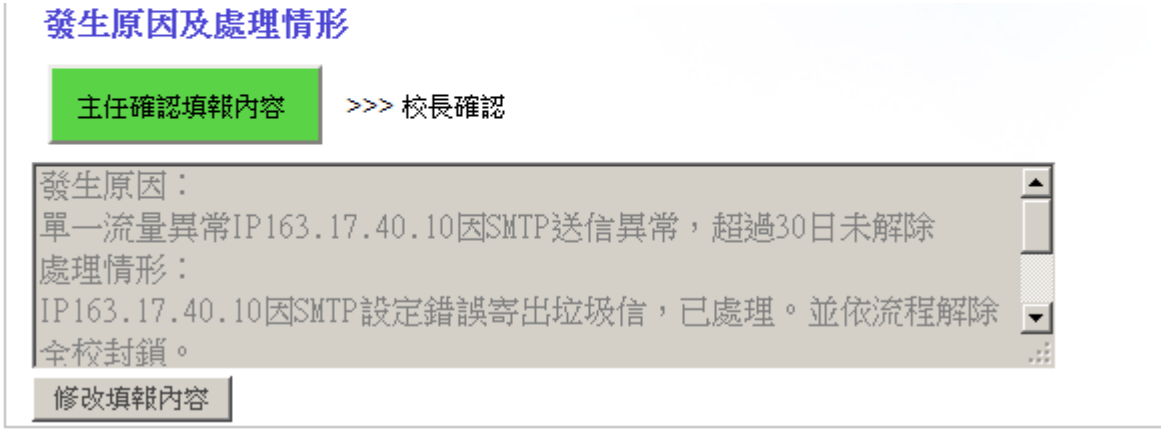
回報流程

1. 登入→具有**資訊組長/網管兼職**的帳號也是貴校事件，會出現及點選「解除」連結

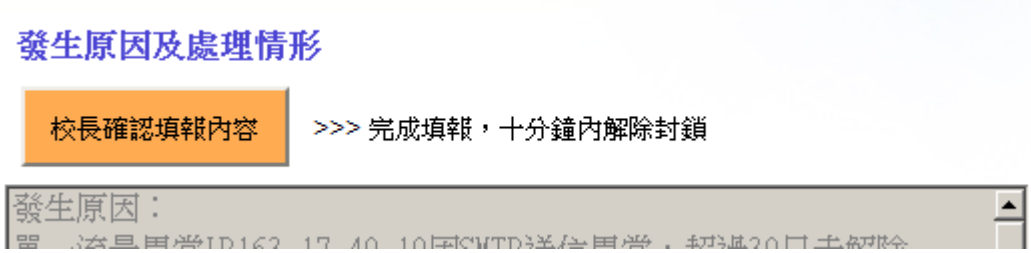


2. 填報原因並按「下一步，主任確認」

3. 請學校主任點選「主任確認填報內容」按鈕
- 主任點選前，資訊組長仍可以修改內容
- 公立高中職(不含市立高中) 僅需填報至主任即可。
- 分校因無校長，請分校填報至主任後請來電解除。



4. 請校長點選「校長確認填報內容」 → 系統於 10 分鐘後自動解除封鎖



十、網域變更

tcc.edu.tw 網域(及以下所屬網域)預計使用到今年底(101.12.31)，請原台中縣學校在年底前轉移至 TC 網域

tceb.edu.tw 網域已停止接受申請，並慢慢轉移至 tc.edu.tw

十一、Forti-manager

供防火牆更新及管理使用，申請表已放在教育局首頁 http://www.tc.edu.tw/docs/download/id/2586

申請 Forti-manager 時防火牆相關設定文件：

http://www.tc.edu.tw/docs/download/id/3426

十二、本年度新申請之校務行政資訊系統雲端服務虛擬主機已開設完成，請新申請學校收到啟用信後，於 1 週內連入更改遠端管理之密碼。續用學校管理 ip 申請變更部分已完成變更，請自行測試。