

100年度雲嘉區域網路中心營運持續計畫演練成果報告

情境二

日期：100.09.16



情境內容

- 區網中心演練情境：因第五級強震（牆壁龜裂，煙囪牌坊傾倒），造成部分未置放於固定式機櫃中之通訊設備或核心業務系統主機從高處掉落，且因供電不穩定導致TANet 骨幹網路短暫中斷及核心業務系統暫時無法提供服務等狀況。
- 情境：區網中心核心業務學籍系統主機發生異常，TANet 骨幹電路骨幹電路發生斷訊情形。



演練前會議

- 演練前演練召集人邀集區網維護TANet網路骨幹維運相關人員召開演練前說明會議。
- 演練召集人說明此次營運持續計畫演練內容及目的。



會議進行狀況

- 參與演練人員熱烈討論演練內容及細節。
- 由演練召集人說明其角色扮演及執行程序。



宣佈演練開始

- 會議中負責人員核對演練開始時間。
- 會議討論完畢後，主席正式宣佈演練開始，並請參與演練之人員就定位。



人員疏散

- 地震後人員疏散並進行人數清點。



啟動應變機制

- 緊急處理組召集人依事故評估之結果建請委員會啟動業務持續計畫。
- 資安官(李副校長)宣佈啟動業務持續計畫。



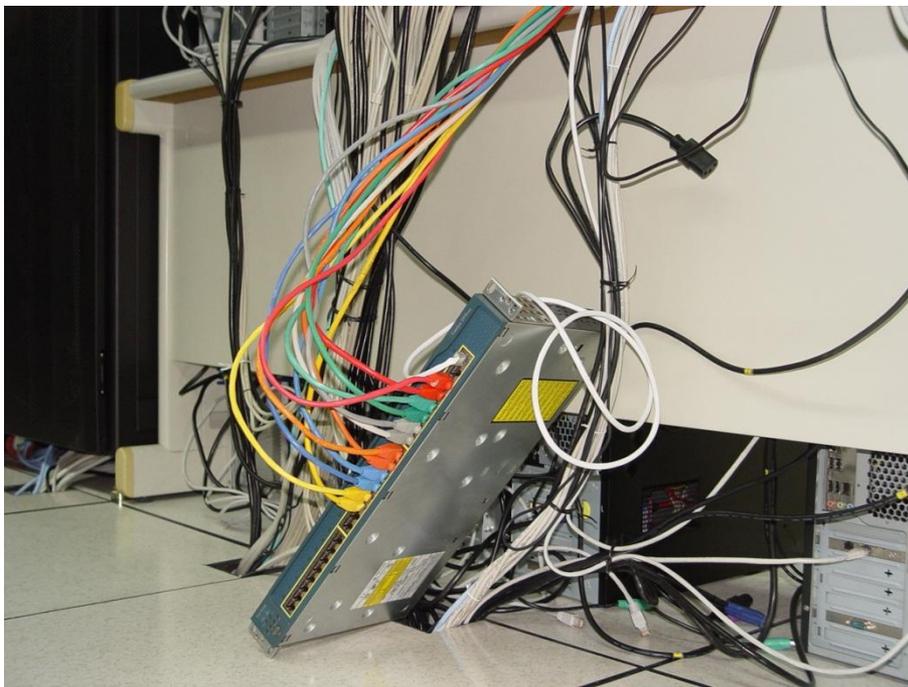
機房設施確認

- 負責人員檢查機房各項環控系統狀況（電力、消防設備、空調、UPS等）。
- 檢測結果環控系統正常。



清查災後損失

- 設備負責人各自清查損失及毀損狀況。
- 清查結果部分資訊設備掉落地板，並發現TANet骨幹電路及學籍系統均異常。



維運人員針對學籍系統伺服器進行檢修

- 維運人員進行狀況了解，同時依『國立中正大學電算中心主機系統管理標準作業流程』進行故障檢修。
- 檢查結果為RAID1之Mirror disk發生故障，導致系統服務異常。



學籍系統伺服器故障復原

- 維運人員以區網備用之同型號磁碟，更換故障之磁碟，同時進行RAID修復。
- 修復同時維運人員連線至伺服器進行確認。



```
140.123.27.247 - PuTTY
root@valkyries # metastat d0
d0: Mirror
  Submirror 0: d10
    State: Okay
  Submirror 1: d20
    State: Okay
  Pass: 1
  Read option: roundrobin (default)
  Write option: parallel (default)
  Size: 12587712 blocks (6.0 GB)

d10: Submirror of d0
  State: Okay
  Size: 12587712 blocks (6.0 GB)
  Stripe 0:
    Device      Start Block  Dbase      State Reloc Hot Spare
    c0t0d0s0    0           No         Okay   Yes

d20: Submirror of d0
  State: Okay
  Size: 12587712 blocks (6.0 GB)
  Stripe 0:
    Device      Start Block  Dbase      State Reloc Hot Spare
    c0t1d0s0    0           No         Okay   Yes

Device Relocation Information:
Device  Reloc  Device ID
c0t0d0  Yes   id1,sd@n5000c50007e98153
c0t1d0  Yes   id1,sd@n5000c50007e717ff
root@valkyries #
```



學籍系統伺服器復原檢測

- 維護廠商到校檢測相關設定，檢測結果顯示正常，學籍系統復原成功，並提供檢測報告單。
- 同時檢測學籍系統連線狀況。




Sitek Technology Inc.
數訊科技股份有限公司
技術服務諮詢表

填表日期: 100年9月16日 表單編號:

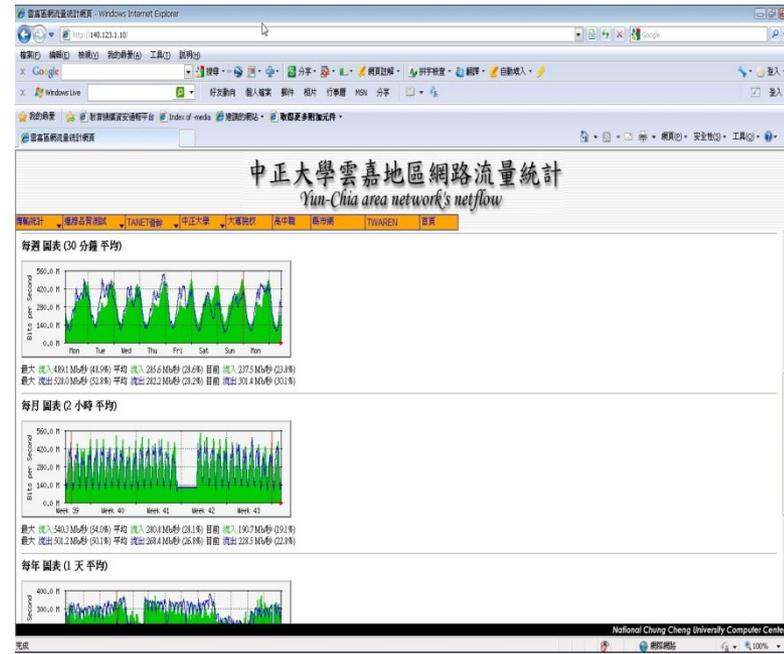
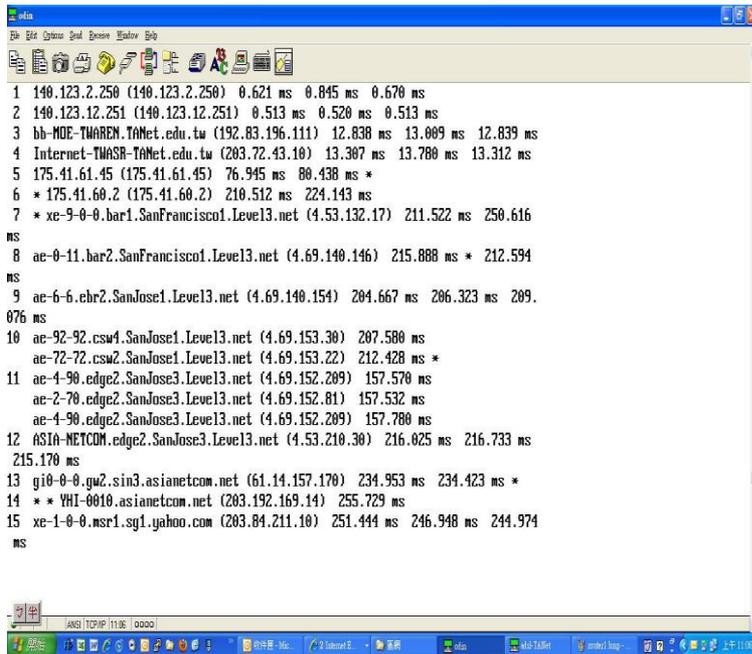
客戶名稱: 中正大學	聯絡人: 郭錦賢	聯絡電話: 2920880					
地址: 嘉義區							
服務類別: <input type="checkbox"/> Contract <input type="checkbox"/> Per Call <input type="checkbox"/> Warranty <input type="checkbox"/> New System <input type="checkbox"/> Add on <input type="checkbox"/> Demo/Test <input type="checkbox"/> Repaired <input type="checkbox"/> Part Replaced <input type="checkbox"/> Unit Swap <input type="checkbox"/> Upgrade <input type="checkbox"/> Adjusted/Cleaned <input type="checkbox"/> Consultant <input type="checkbox"/> P.M. <input type="checkbox"/> Inspection <input type="checkbox"/> Installation <input type="checkbox"/> Other/None							
服務代碼: <input type="checkbox"/> Tape <input type="checkbox"/> Board <input type="checkbox"/> CPU <input type="checkbox"/> Disk <input type="checkbox"/> Printer/Plotter <input type="checkbox"/> Monitor <input type="checkbox"/> Memory <input type="checkbox"/> Environment <input type="checkbox"/> Audio <input type="checkbox"/> Keyboard/Mouse <input type="checkbox"/> Power Supply <input type="checkbox"/> Frame Buffer <input type="checkbox"/> Language <input type="checkbox"/> Networking <input type="checkbox"/> Graphic/Window 代碼: <input type="checkbox"/> System S/W <input type="checkbox"/> System H/W <input type="checkbox"/> Application S/W <input type="checkbox"/> System/Network Management <input type="checkbox"/> Utility <input type="checkbox"/> Others							
機型號碼: _____	序號: _____	問題登錄 月 日: _____					
收費明細: <input type="checkbox"/> 收費 <input type="checkbox"/> 免費	完成狀況: <input type="checkbox"/> 未完成 <input type="checkbox"/> 已完成	回應時間 月 日: _____					
問題描述: 因5級地震造成不更硬碟損毀		線上解決 月 日: _____					
		聯絡工程師 月 日: _____					
		出發時間 月 日: _____					
		到達時間 9月16日 14:30					
		完成時間 9月16日 14:50					
		退班時間 月 日: _____					
		歸案時間 月 日: _____					
		確認時間 月 日: _____					
工作內容: 1. 等理者已更換備用硬碟 2. 系統狀態檢測OK 3. 系統記錄檢查OK							
新裝零件		原裝零件					
Part Number	Serial Number	Rev.	Description	Part Number	Serial Number	Rev.	Description
維修工程師簽署: 葉成茂				客戶簽署: 郭錦賢 9/16			
說明: 一、本表一式三聯: (一)本公司留存一白聯 (二)客戶留存一紅聯 (三)本公司經辦人留存一綠聯 二、計時服務以到服務地點時間開始計算至停運結束時間止。 三、逾時不滿一小時以一小時計算。 四、收費項目依照本公司維護費用報價說明。							

客戶服務中心處理辦法 <S025-01>100.04.1.000



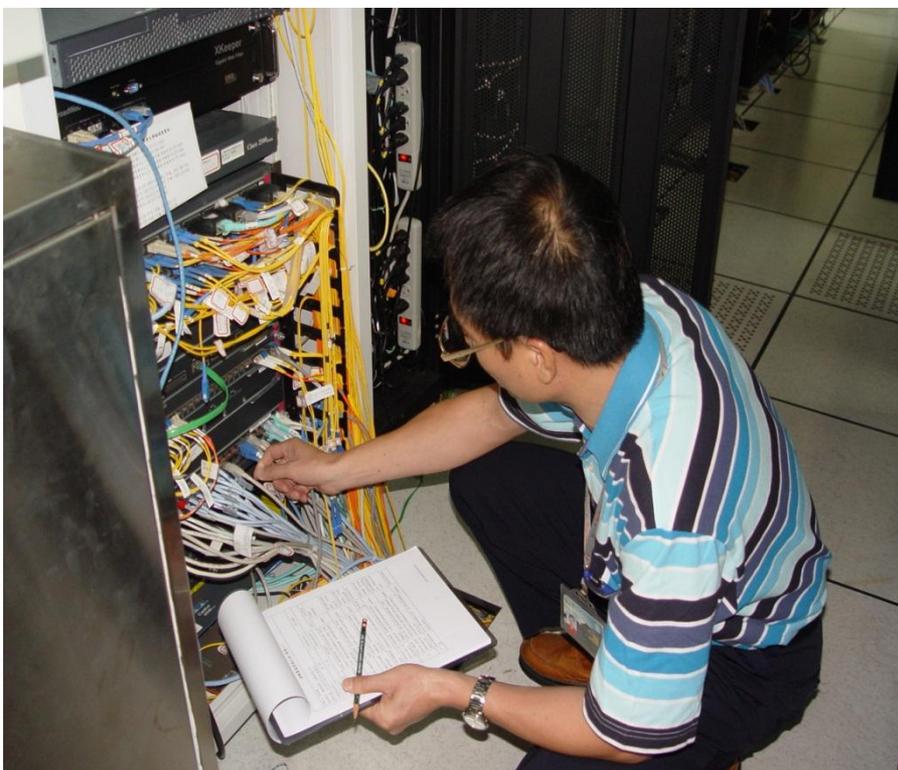
TANet 電路狀況監測

- TANet 骨幹負責人，以 netmon 指令及 Mrtg 流量監測系統檢測骨幹電路狀況。
- 檢測結果發現，骨幹電路流量異常。



路由器網路狀態檢查

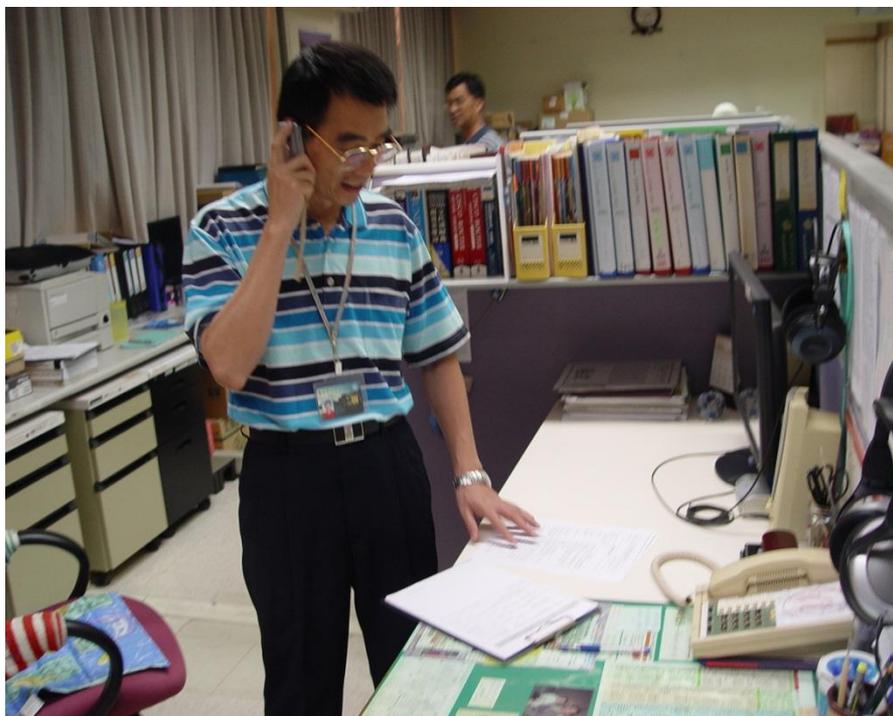
- 機房中檢查線路狀況，並連線至路由器檢視網路通訊介面 (slot port) 狀態及路由設定。
- 檢查結果發現路由器正常，推斷為中華電信骨幹電路問題。



```
mlst-TANet
File Edit Options Send Receive Window Help
[Icons]
TANET_CCU_C6Kwsh int gigabitEthernet 6/8
GigabitEthernet6/8 is administratively down, line protocol is down (disabled)
Hardware is C6k 1000Mb 802.3, address is 0007.ec6e.b000 (bia 0007.ec6e.b000)
Description: tanet-1
MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 1000Mb/s
input flow-control is off, output flow-control is off
Clock mode is auto
ARP type: ARPA, ARP Timeout 04:00:00
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes): Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicasts)
    0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 0 multicast, 0 pause input
```

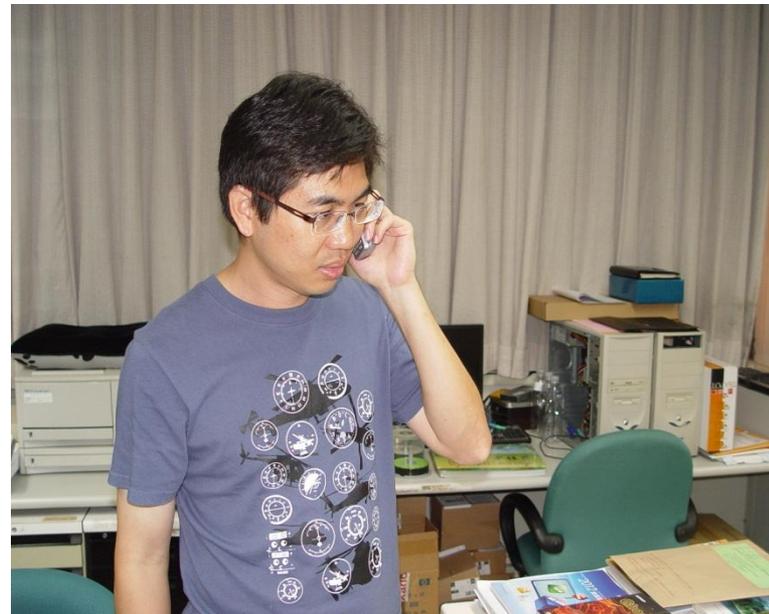
通報TANet 電路維護廠商

- 以電話通知TANet電路維護廠商(中華電信維運機房)，請其儘速進行電路修復。



進行資安通報

- 維運人員判定為資訊安全事件，並以電話通知資訊安全官及單位主管，報告學籍系統伺服器及骨幹電路狀況。
- 同時以簡訊或電話通報區網下游連線單位。



資訊安全事件報告單(1/2)

- 由區網網路維運人員依現況填報資安訊安全事件報告單，並由資訊安全官簽核。

資訊安全事件報告單					
文件編號	RNC-CCU-D-035	機密等級	限閱	版次	1.2
紀錄編號：100-05		填表日期：100年9月16日			
一、發生資訊安全事件之單位聯絡資料：					
單位名稱：國立中正大學電算中心		通報人：郭錦賢			
電話：05-2720480		傳真：05-2720485		E-mail：jsguo@ccu.edu.tw	
二、資訊安全事件通報事項：					
1.事件發生時間：100年9月16日14時00分					
2.設備資料：					
◎IP 位址 (IP Address)：_____ (無：可免填)					
◎網際網路位址 (Web-URL)：_____ (無：可免填)					
◎設備廠牌、機型：中華電信幹線					
◎作業系統名稱、版本：TANet 網路骨幹					
◎已裝置之安全機制：_____					
3.資訊安全事件資料：					
◎事件等級： <input type="checkbox"/> 4級； <input type="checkbox"/> 3級； <input checked="" type="checkbox"/> 2級； <input type="checkbox"/> 1級； <input type="checkbox"/> 0級					
4級： <input type="checkbox"/> 國家機密資料遭洩漏					
<input type="checkbox"/> 國家重要資訊基礎建設系統或資料遭竄改					
<input type="checkbox"/> 國家重要資訊基礎建設運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作。					
3級： <input type="checkbox"/> 密級或敏感公務資料遭洩漏					
<input type="checkbox"/> 核心業務系統或資料遭嚴重竄改					
<input type="checkbox"/> 核心業務系統或資料遭輕微竄改。					
<input checked="" type="checkbox"/> 核心業務運作遭影響或系統效率降低，於可容忍中斷時間內回復正常運作。					
2級： <input type="checkbox"/> 非屬密級或敏感之核心業務資料遭洩漏					
<input type="checkbox"/> 核心業務系統或資料遭輕微竄改。					
<input checked="" type="checkbox"/> 非核心業務運作遭影響或短暫停頓。					
1級： <input type="checkbox"/> 非核心業務資料遭洩漏。					
<input type="checkbox"/> 非核心業務系統或資料遭竄改。					
<input type="checkbox"/> 非核心業務運作遭影響或短暫停頓。					
◎事件說明：(文字勿超過100中文字，標點符號請用大寫)					
◎可能影響範圍及損失評估：(文字勿超過100中文字，標點符號請用大寫)					
◎應變措施：(文字勿超過100中文字，標點符號請用大寫)					
三、期望支援項目：希望電路提供廠商隨時保持電路狀況監控，確保網路暢通及使用者權益。					
四、解決辦法：進行電路搶修作業後運作回復正常。					
五、已解決時間：100年9月16日15時10分					
權責單位	會辦	單位	資訊安全官		
郭錦賢		郭錦賢			
[簽名]		[簽名]			

安全事件管理程序書



資訊安全事件報告單(2/2)

- 由學藉系統負責人
員依現況填報資安
訊安全事件報告單，
並由資訊安全官簽
核。

資訊安全事件報告單					
文件編號	RNC-CCU-D-035	機密等級	限閱	版次	1.2
紀錄編號：100-06		填表日期：100年9月16日			
一、發生資訊安全事件之單位聯絡資料：					
單位名稱：國立中正大學電算中心		通報人：陳恩翰			
電話：05-2720480		傳真：05-2720485		E-mail：shchen@ccu.edu.tw	
二、資訊安全事件通報事項：					
1. 事件發生時間：100年9月16日14時30分					
2. 設備資料：					
◎IP位址 (IP Address)：140.123.30.8 (無；可免填)					
◎網際網路位址 (Web-URL)： (無；可免填)					
◎設備廠牌、機型：Sun M5000					
◎作業系統名稱、版本：Solaris 10					
◎已裝置之安全機制： (無；可免填)					
3. 資訊安全事件資料：					
◎事件等級： <input type="checkbox"/> 4級； <input type="checkbox"/> 3級； <input checked="" type="checkbox"/> 2級； <input type="checkbox"/> 1級； <input type="checkbox"/> 0級					
4級： <input type="checkbox"/> 國家機密資料遭洩漏					
<input type="checkbox"/> 國家重要資訊基礎建設系統或資料遭竄改					
<input type="checkbox"/> 國家重要資訊基礎建設運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作。					
3級： <input type="checkbox"/> 密級或敏感公務資料遭洩漏					
<input type="checkbox"/> 核心業務系統或資料遭嚴重竄改					
<input type="checkbox"/> 核心業務運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作					
2級： <input type="checkbox"/> 非屬密級或敏感之核心業務資料遭洩漏					
<input type="checkbox"/> 核心業務系統或資料遭輕微竄改。					
<input checked="" type="checkbox"/> 核心業務運作遭影響或系統效率降低，於可容忍中斷時間內回復正常運作。					
1級： <input type="checkbox"/> 非核心業務資料遭洩漏。					
<input type="checkbox"/> 非核心業務系統或資料遭竄改。					
<input type="checkbox"/> 非核心業務運作遭影響或短暫停頓。					
◎事件說明：(文字勿超過100中文字，標點符號請用大寫)					
◎可能影響範圍及損失評估：(文字勿超過100中文字，標點符號請用大寫)					
◎應變措施：(文字勿超過100中文字，標點符號請用大寫)					
三、期望支援項目：據上述演練執行項目、程序及結果，作為爾後學籍系統伺服器故障偵測、排除及復原等程序之參考。					
四、解決辦法：經更換故障磁碟機及 RAID 修復後系統回復正常。					
五、已解決時間：100年9月16日14時50分					
權責單位	會辦	單位	資訊安全官		
陳恩翰			李新林		

1

安全事件管理程序書



TANet 骨幹維護廠商接獲通知

- 中華電信公司接獲電話通知電路異常狀況。
- 廠商派員進行電路整體檢查、修復及問題處理。

欄位名稱	欄位資料
是否影響服務	否
STM64系統名稱	CAUV-HY01-STM64-2 (中正大學(電算中心),國家網路中心1F,STM64系統,2)
起始時間	2011-09-16 14:00
終止時間	2011-09-16 16:00
填寫時間	2011-09-09 11:30
申報時間	2011-09-09 11:30
指揮中心	台南營運處澎湖工務課網路股
填寫人員	嘉義營運處 局內網路中心 李坤城 (電話:05-2444298 手機:0910896740)
改接/傳輸負責人	臺南營運處 澎湖服務中心 陳宏輝 (電話:06-9440514 手機:0910374450)
線路負責人	嘉義營運處 局內網路中心 李坤城 (電話:05-2444298 手機:0910896740)
申報人員	嘉義營運處 局內網路中心 李坤城 (電話:05-2444298 手機:0910896740)
地點	中正大學(電算中心)
原因	配合中正大學地震防災演練中華電信電路自動切換
公文文號	



廠商回報修復記錄

- 廠商將電路修復後，同時以電話報告修復狀況，並提供修復紀錄表。

企客等級:1 / 國立中正大學

10G 專線 5226E - 80015- 目前沒有申告

100/09/16 14:35~15:10 演練期間，

中華電信 ROADM 環路自動切換路由，電路正常，無中斷服務。

台灣南區電信分公司 嘉義電信營運處 局網三股 李坤城



TANet 骨幹復原測試

- 維運人員進行網路測試，確認廠商確實已完成電路修復。



```
Hardware is C6k 1000Mb 802.3, address is 0018.b9d2.a2c0 (bia 0018.b9d2.a2c0)
Description: tanet-1
MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 16/255, rxload 85/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 1000Mb/s, media type is LH
input flow-control is off, output flow-control is off
Clock mode is auto
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:34, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 169108
Queueing strategy: fifo
Output queue: 0/40 (size/max)
30 second input rate 333927000 bits/sec, 43918 packets/sec
30 second output rate 66360000 bits/sec, 22724 packets/sec
933119199932 packets input, 776823153352927 bytes, 0 no buffer
Received 106151439 broadcasts (106114316 multicasts)
 0 runs, 0 giants, 0 throttles
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
 0 watchdog, 0 multicast, 0 pause input
 0 input packets with dribble condition detected
904952745485 packets output, 309680787447251 bytes, 0 underruns
```



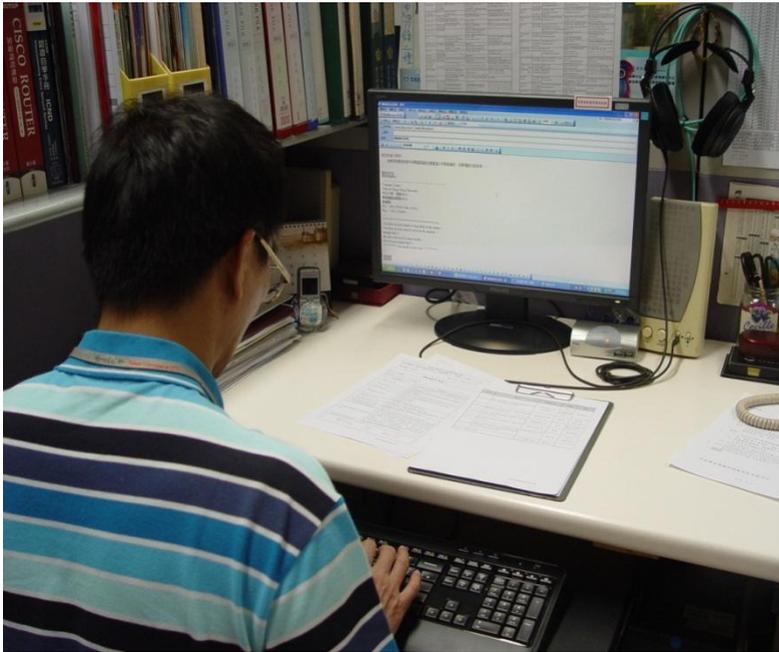
事件處理回報 (1/2)

- 各系統負責人員向資訊安全官(李副校長)回報事件處理狀況。



事件處理回報 (2/2)

- 以E-Mail或電話通報區網下游連線單位電路異常狀況解除。



總結報告與檢討

- 資訊安全官李副校長親自主持演練總檢討會議。
- 演練執行項目、程序及結果，做為日後學籍系統及骨幹電路異常、排除及復原等程序之參考。

