

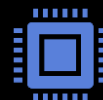


宜蘭區網中心  
ILAN REGIONAL CENTER

## 簡報項目



資安平台預警單處理



資安平台增設功能

# ※資安平台預警單處理

回首頁

修改個人資料

登出

通報

通報/應變

自行通報

事件單處理狀態

歷史通報

帳號管理

事件附檔下載

資安預警事件

事件統計

演練資訊

情資資料下載

事件單編號	發佈時間	距通報時間(小時)	流程
-------	------	-----------	----

Page 1/1

尚有23張EWA預警單未處理，請按此查閱相關資訊

# ※資安平台預警單處理 各預警單查詢

回首頁

修改個人資料

登出

通報

通報/應變

自行通報

事件單處理狀態

歷史通報

帳號管理

事件附檔下載

資安預警事件

事件統計

演練資訊

情資資料下載

事件編號:

狀態:

所有

查詢

第一頁

| 上一頁

| 下一頁

| 最終頁

EWA編號	單位名稱	事件等級	事件分類	狀態	LOG
<a href="#">NTUSOC-EWA-201910-0385</a>	國立宜蘭大學	2	可疑連線	未處理	下載
<a href="#">NTUSOC-EWA-201905-0504</a>	國立宜蘭大學	low	可疑連線	未處理	下載
<a href="#">NTUSOC-EWA-201905-0434</a>	國立宜蘭大學	low	可疑連線	未處理	下載
<a href="#">NTUSOC-EWA-201905-0369</a>	國立宜蘭大學	low	可疑連線	未處理	下載
<a href="#">NTUSOC-EWA-201905-0225</a>	國立宜蘭大學	low	可疑連線	未處理	下載
<a href="#">NTUSOC-EWA-201905-0151</a>	國立宜蘭大學	low	可疑連線	未處理	下載
<a href="#">NTUSOC-EWA-201905-</a>	國立宜蘭大學	low	可疑連線	未處	下載





# ※資安平台預警單處理 預警單所呈現內容

回首頁 改個人 登出 通報 通報/應 自行通 生單處理 歷史通 帳號管 安預警 事件統 演練資 資資料

聯絡電話: 039317129# E-Mail: chihchieh@niu.edu.tw  
聯絡電話: 07-525-0211 E-Mail: service@cert.tanet.edu.tw

close or Esc Key

EWA事件單	
事件編號	NTUSOC-EWA-201910-0385
單位名稱	國立宜蘭大學
發佈時間	2019-10-07 08:10:15
發生時間	2019-10-06 21:15:53
受害IP	120.101.36.148

大學 王管機關: 宜蘭區域網路中心 聯絡電話: 039317129# E-Mail: chihchieh@niu.edu.tw  
教育機構資安通報應變小組 聯絡電話: 07-525-0211 E-Mail: service@cert.tanet.edu.tw

close or Esc Key

應變措施	請檢視來源IP該連線行為是否已得到合法授權。若來源IP該連線為異常行為，可先利用掃毒軟體進行全系統掃描，並利用ACL暫時阻擋該可疑IP。同時建議管理者進行以下檢查。	
參考資訊	NULL	

→

EWA事件單狀態		
<input type="radio"/> 誤判		
<input type="radio"/> 確實事件	事件單編號	
<input type="radio"/> 無法判斷		
原因		

送出

預警單為 **TACERT** 無法確認之事件單，需透過自校查詢確認來判斷如何填報

回首頁

修改個人資料

登出

通報

通報/應變

自行通報

事件單處理狀態

歷史通報

帳號管理

事件附檔下載

資安預警事件

事件統計

演練資訊

情資資料下載

填報時間為:2019-11-4 11:2:11

## 通報流程

各機關因受外在因素所產生資通安全事件時通報事項：

以下表單各欄位若為紅色⊙標示，則為必填欄位  
欄位中不得輸入特殊符號，例如：「;」、「"」、「'」、「\$」、「&」、「%」、「!」、「^」、「\*」、「<」、「>」、「\_」、「|」、「-」

1. 通報型態: **■主動通報(各單位自行發現資安事件)**

2. ⊙事件發生時間:

⊙IP位置 (IP address) :   
範例: 120.114.22.33

⊙網際網路位置 (web-url) :   
範例: https://www.xxx.edu.tw/cba.index

⊙設備廠牌、機型:   
範例1: 華碩 TS100 E6  
範例2: Acer AT110 F1

⊙作業系統 (名稱/版本):   
範例1: Centos Linux 5.4,  
範例2: Windows XP SP2

⊙受駭應用軟體 (名稱/版本):   
範例: sendmail server, 此為不確定版本的範例

⊙已裝置之安全防護軟體:  
防毒軟體 (名稱/版本):   
範例: Avira 10.0.0.561

# ※資安平台預警單處理 預警事件相關資訊查詢

回首頁

修改個人資料

登出

通報

通報/應變

自行通報

事件單處理狀態

歷史通報

帳號管理

事件附檔下載

資安預警事件

事件統計

演練資訊

情資資料下載

事件編號:  狀態: 所有

第一頁 | 上一頁 | 下一頁 | 最終頁

EWA編號	單位名稱	事件等級	事件分類	狀態	LOG
<a href="#">NTUSOC-EWA-201910-0385</a>	國立宜蘭大學	2	可疑連線	未處理	下載
<a href="#">TACERT-EWA-201908-00027</a>	國立宜蘭大學	1	其他	確實事件	下載
<a href="#">NTUSOC-EWA-201905-0504</a>	國立宜蘭大學	low	可疑連線	未處理	下載
<a href="#">NTUSOC-EWA-201905-0434</a>	國立宜蘭大學	low	可疑連線	未處理	下載
<a href="#">NTUSOC-EWA-201905-0369</a>	國立宜蘭大學	low	可疑連線	未處理	下載
<a href="#">NTUSOC-EWA-201905-0225</a>	國立宜蘭大學	low	可疑連線	未處理	下載
<a href="#">NTUSOC-EWA-201905-</a>	國立宜蘭大學	low	可疑連線	未處理	下



# ※資安平台增設功能 改善措施

## 增設 改善措施 項目

目的：主要為了符合實際處理狀態及時間，並符合資安法規範

### 6. 是否需要支援?

- 是  否:通報單位自行解決
- 你的上層機關負責人為: 莊智傑  
聯絡電話:039317129#  
E-mail:chihchieh@niu.edu.tw  
期望支援方式:  
 電話告知  Email告知

### 7. 是否同時進行通報流程與應變流程?

- 是 (請繼續完成 II.應變流程之作業)  否 (會先完成 I.通報流程 並結束，後續時間請儘快完成 II.應變流程)

## 應變流程

1. 緊急應變措施  已中斷網路連線，待處理完成後再上線  
 已停止伺服器之服務，待處理完成後再上線  
 直接處理完成，解決辦法詳見【解決辦法】  
 其它

2. 解決辦法： (文字勿超過200中文字，標點符號請用全形)

3. 解決時間：

## 改善措施

- 改善辦法： (文字勿超過200中文字，標點符號請用全形)

依資通安全相關管理規範進行改善措施

- 改善時間：

發佈通報



簡報結束 感謝聆聽



宜蘭區網中心  
ILAN REGIONAL CENTER