# 教育機構資安通報應變平台 v3 新功能介紹與操作手冊

教育機構資安通報平台根據各位平台使用者的反應以及建議，已於日前已完成了新功能的開發作業。此次平台主要的新增功能為：

(1) **事件附檔下載**：連線單位資安人員將可於平台上，即時下載資安事件單與資安預警(EWA)事件單的佐證資料，加速事件處理的效率。

(2) **EWA 事件管理**：新版教育機構資安通報平台已與資安預警(EWA)管理平台整合。日後連線單位的資安人員在處理完資安預警事件(EWA)後，不需再回報所屬區縣市網路中心。由連線單位的資安人員自行登入教育機構資安通報平台後，變更 EWA 事件單的狀態即可。

(3) **通報平台顯示資訊部分調整**：調整資安通報平台部分之顯示資訊，讓使用者更方便操作與瀏覽事件單狀態。

## 一、 「事件附檔下載」功能說明

步驟 1：確認欲下載事件單的『發佈編號』。

- 資安事件單的發佈編號：點入『通報 / 應變』功能區後，即可看到待處理事件單，點擊事件單編號後，即可看到完整的事件單內容，而『發佈編號』就在上方的第二個欄位中。


- 資安預警事件的發佈編號：點入左方的『EWA 事件』功能區後，即可看到待處理的資安預警事件列表。**EWA 編號即是『發佈編號』。**

步驟 2. 下載事件附檔：至左方的『事件附檔下載』功能區，根據『發佈編號』，點選後方的功能鈕『下載』，即可得到原發單單位的佐證資料。


## 二、 EWA(資安預警)事件處理功能說明：

資安預警情資(EWA)規劃的重點在於強調預警的功能。當有跡象顯示資安事件即將發生或是已發生但無明確證據顯示時，為避免事件繼續擴大，造成更大損失，因此才規劃此資安預警情資(EWA)。也因為部份資安事件的分析技術需要更多各單位的系統資訊及各種確認資訊才可更加明確，所以資安預警情資(EWA)有部份可能因證據不足而存在誤判情況，懇請諸位資安先進多加費心處理資安預警情資。

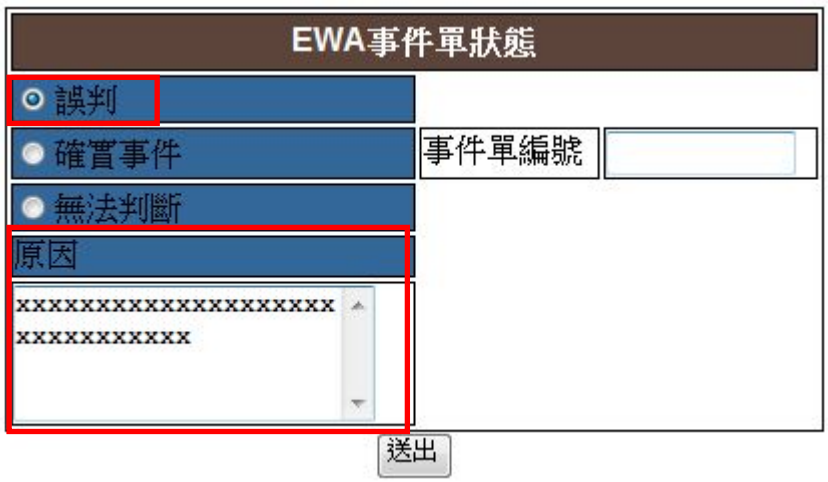
步驟一：點選 EWA 事件：可瀏覽單位內所有的 EWA 事件單。


步驟二：回報 EWA 處理狀態：點選 EWA 編號可顯示完整 EWA 事件單訊息，請於「EWA 事件單處理狀態」進行處理回報。

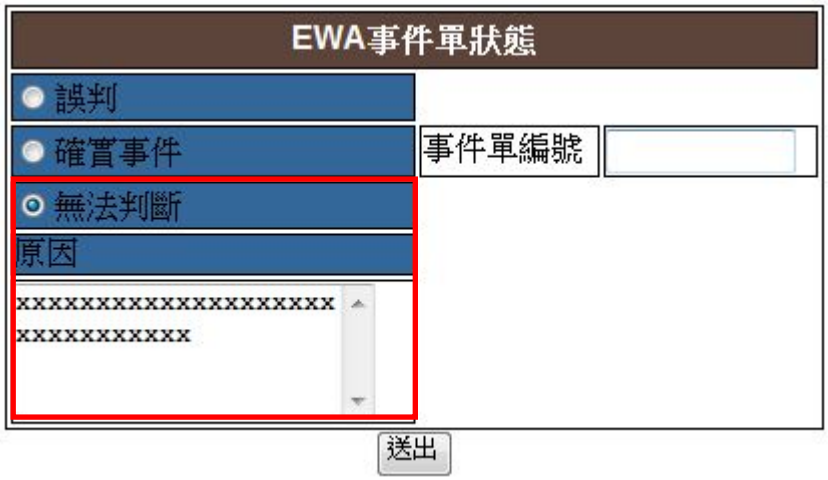
EWA 處理狀況分三種：

(1) **確實事件**：經查證後為確實事件，請先進行「自行通報」，接著於該 EWA 事件單狀態點選「確實事件」，並於後方「事件單編號」填入自行通報的資安事件編號。


(2) **誤判**：經查證後確認為誤判事件，請於 EWA 事件單狀態點選「誤判」，並於下方「原因」欄位中，說明誤判原因。




(3) **無法判斷**：經查證後確認為無法判斷事件，請於 EWA 事件單狀態點選「無法判斷」，並於下方「原因」欄位中，說明無法判斷原因。




## 三、 通報平台顯示資訊部分調整：

1. 首頁或選取「通報/應變」即顯示出所有待通報及待應變的事件單資訊，可直接點選事件單編號進行通報與應變流程。

2. 點選「事件單處理狀態」，可顯示所有尚未結案(二線區縣市網及三線資安通報小組中心尚未完成審核)的事件單狀態，新增顯示「技術支援」欄位，方便二線區縣市網中心人員查看。(注意，於事件單處理狀態中無法進行填寫通報與應變流程)


3、點選「歷史通報」，可查詢到所有已結案之事件單，顯示資訊新增「IP 欄位」，與事件單「發佈時間」及「結案時間」，方便各單位進行事件單追查。


教育機構資安通報平台
Ministry of education information & communication security contingency platform
TANet CERT
聯絡資訊
機關名稱:
使用者:
主管機關:
聯絡電話:
E-Mail:
教育機構資安通報應變小組
聯絡電話:07-525-0211
E-Mail:
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
事件附檔下載
EWA事件
工單狀態
事件單編號
單位
來源
等級
IP
發佈時間
結案時間
129
自行
2級
.30
2011-10-28 15:15:07
2011-10-28 15:25:34
8
NTU
3級
.123
2011-10-28 10:53:54
2011-10-28 11:37:41
4
G-ISAC
2級
.123
2011-10-28 10:53:54
2011-10-28 11:30:26
Page 1/1