

教育機構資安通報

- 登入

- ✓ <https://info.cert.tanet.edu.tw/>
- ✓ 帳號：組織與團體物件識別碼 (OID)。
- ✓ 密碼：若忘記可依網站指示聯絡 TACERT 客服人員。

- 填報時機

- ✓ 自行通報：自行發現或資訊中心通知必須上網填報時。
- ✓ 告知通報：接到資安通報中心的告知通報時。
- ✓ 資安預警：接到資安通報中心的資安預警通知 (EWA) 時。

- 佐證資料

- ✓ 事件附檔下載：告知通報與資安預警的「證據」檢視。

自行 / 告知通報填寫注意事項

在「7.◎ 是否同時進行通報流程與應變流程？」這問題一定要答「是」，並繼續填寫「應變流程」再「發佈通報」

<p>回首頁</p> <p>修改個人資料</p> <p>登出</p> <p>通報</p> <p>通報/應變</p> <p>自行通報</p> <p>事件單處理狀態</p> <p>歷史通報</p> <p>事件附檔下載</p> <p>資安預警事件</p>	<p>填報時間為:2012-9-24 18:21:11</p> <h3>通報流程</h3> <p>各機關因受外在因素所產生資通安全事件時通報事項：</p> <p>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：「;」、「"」、「'」、「\$」、「&」、「%」、「!」、「^」、「*」、「<」、「>」、「_」、「 」、「-」</p> <p>1. 通報型態: <input checked="" type="checkbox"/> 主動通報(各單位自行發現資安事件)</p> <p>2. ◎事件發生時間: <input type="text"/></p> <p>◎IP位置 (IP address) : <input type="text"/> 範例: 120.114.22.33</p>
---	---



自行 / 告知通報填寫注意事項



7. 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

①1. 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

②2. 解決辦法： (文字勿超過200中文字，標點符號請用全形)

③3. 解決時間：

發佈通報

一定要填「是」

再把右邊流程填寫完

資安預警事件 (一)

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
資安預警事件

EWA編號	單位名稱	事件等級	事件分類	狀態
ASOC-EWA-201209-1075	台南市網中心	low	對外攻擊	誤報

Page 1/1

資安預警事件 (二)

The screenshot displays a web interface for managing security alerts. It is divided into three main sections:

- Top Section (EWA事件單):** Shows a list of events. The first entry has the ID "ASOC-EWA-201209-1075". A blue callout bubble with the text "先把編號複製起來" (Copy the ID first) points to this ID.
- Middle Section (參考資訊):** A window titled "close or Esc Key" containing a reference link: "本攻擊相關資訊可於下列網址http://www.iss.net/security_center/reference/vuln/icmp_flood.htm內查詢". A large red arrow points from the ID in the top section down to this section.
- Bottom Section (EWA事件單狀態):** A form for updating the event status. The "事件單編號" (Event ID) field contains "ASOC-EWA-201209-1075". A red arrow points from the ID in the top section to this field with the text "把編號貼上" (Paste the ID). The "原因" (Reason) field contains "該 IP 已停用" (This IP is disabled). A red circle highlights the radio button options: "誤判" (Selected), "確實事件" (Confirmed event), and "無法判斷" (Cannot determine). To the left of this section, the text "依實況填寫" (Fill in according to actual situation) is written vertically. A "送出" (Submit) button is at the bottom.

事件附檔下載

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

資安預警事件

工單狀態

輸入事件單、EWA發佈編號或事件單編號

搜尋

時間	發佈編號	IP	單位	來源	LOG附檔
Sun 23, Sep 2012	ASOC-EWA-201209-1075 (資安預警事件的證據)	163.26.176.4	台南市網中心	S-ASOC	下載
Wed 27, Jun 2012	TACERT-DEF-201206-0164 (告知通報的證據)	163.26.87.195	台南市網中心	TACERT	下載

Page 1/1

台灣學術網路危機處理中心(TACERT)