# 教育機構資安回饋平台-
# DDoS 清洗系統操作手冊
# V2 版

TACERT 臺灣學術網路危機處理中心團隊 製

2019/12

# 目錄

## 一、 前言

現今的網路攻擊日益頻繁，規模更大，且複雜度更勝以往。尤其近年來國際間發生多起大規模 DDoS(Distributed Denial of Service ,分散式阻斷服務攻擊)攻擊事件，而且攻擊規模更頻頻創新高。有鑑於此，教育部已於 S-ASOC 及 N-ASOC 建置 TANet 流量清洗中心，當 TANet 內部單位遭受 DDoS 攻擊時，可透過 TANet 流量清洗中心過濾掉攻擊封包，讓系統可迅速回復正常。TACERT 團隊負責開發「DDoS 清洗系統」以協助二線區縣市網路中心人員以及 SOC 團隊申請 DDoS 清洗服務以及管理清洗流程進度使用，

「DDoS 清洗系統」目前僅提供二線區縣市網路中心以及 SOC 團隊使用，若學術單位遭受 DDoS 攻擊時，請透過其所屬之區縣市網路中心申請流量清洗服務。教育體系 DDoS 攻擊清洗申請流程表依圖 1 所示，當 DDoS 攻擊清洗完成後，平台會自動產生一張告知通報事件單，連線單位需登入資安通報平台進行填寫通報應變措施，才算完成整個 DDoS 攻擊清洗申請流程。

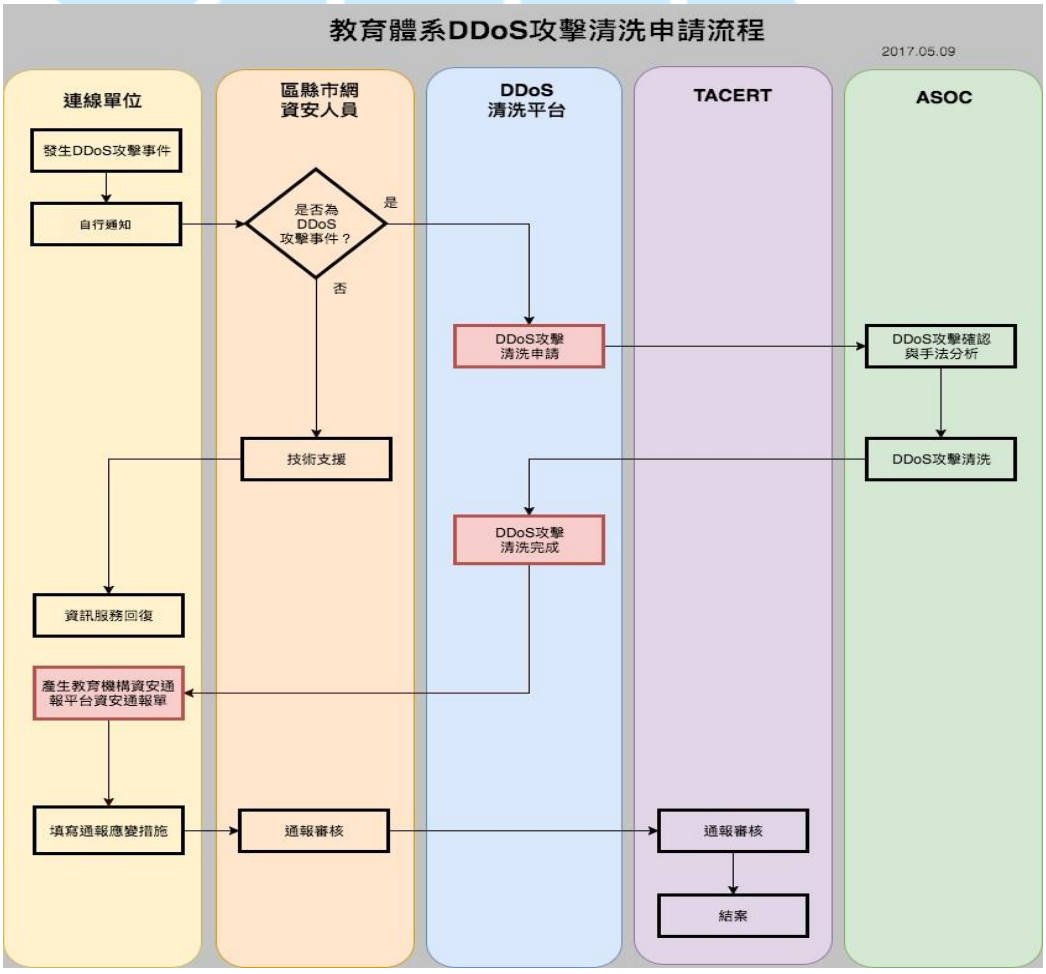


圖 1 教育體系 DDoS 攻擊清洗申請流程

## 二、 系統說明

為方便二線區縣市網路中心人員以及 SOC 團隊人員使用，TACERT 團隊將「DDoS 清洗系統」整合進「教育機構資安通報回饋平台」，使用者只需登入回饋平台即可使用此服務。

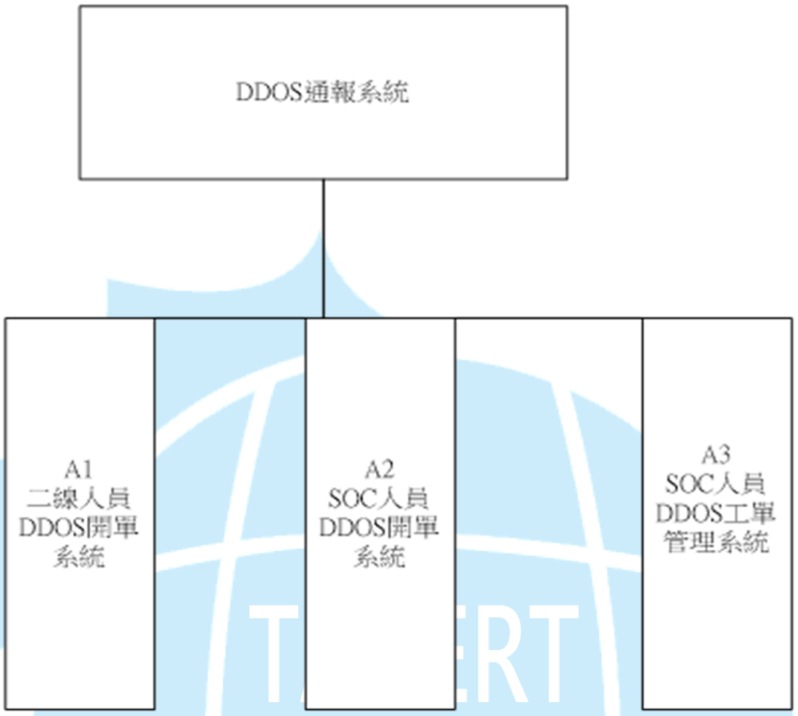


圖 2 DDoS 清洗作業系統功能表

| 功能 | 功能說明 |
|---|---|
| A1-二線人員 DDOS 開單系統 | 提供權限登入及新增、查詢 DDOS 工單功能 |
| A2- SOC 人員 DDOS 開單系統 | 提供權限登入及新增、查詢 DDOS 工單功能 |
| A3- SOC 人員 DDOS 管理系統 | 提供管理二線人員 DDOS 工單功能 |

表 1 DDoS 清洗作業系統功能說明

## 三、 操作說明(二線區縣市網路中心人員)

下列將針對系統及子功能進行操作說明，並佐以畫面以利操作。

### (1) 系統網址及登入說明

①系統網址：https://portal.cert.tanet.edu.tw

選擇「**資安通報報表系統**」，如圖 3。


圖 3 資安通報報表系統界面

②於登錄畫面鍵入帳號、密碼及驗證碼，如圖 4。


圖 4 登錄介面

### (2) 新增 DDoS 清洗服務申請

①登入資安通報報表系統平台後先點選上方工作列「DDOS 清洗系統」，再點選「新增申請單」。


圖 5 資安通報報表系統登錄後的界面

②產生如圖 6 所示的表單，平台會自動篩選出其轄下的連線單位列表供使用者選擇，使用者將相關資訊(*為必填欄位)填入「送出」即可。


圖 6 DDOS 清洗申請單表單內容

**(3) 檢視 DDoS 工單資訊**

①點選「DDOS 清洗系統」功能將顯示所有 DDOS 工單資訊，其中「狀態」說明如下

狀態:待處理（二線人員新增 DDOS 工單）

處理中(SOC 人員正在處理)

處理完成並在保護中(已處理完成)

處理完成並已移出保護中(已處理完成)

失敗(SOC 處理該工單失敗,無法清洗)

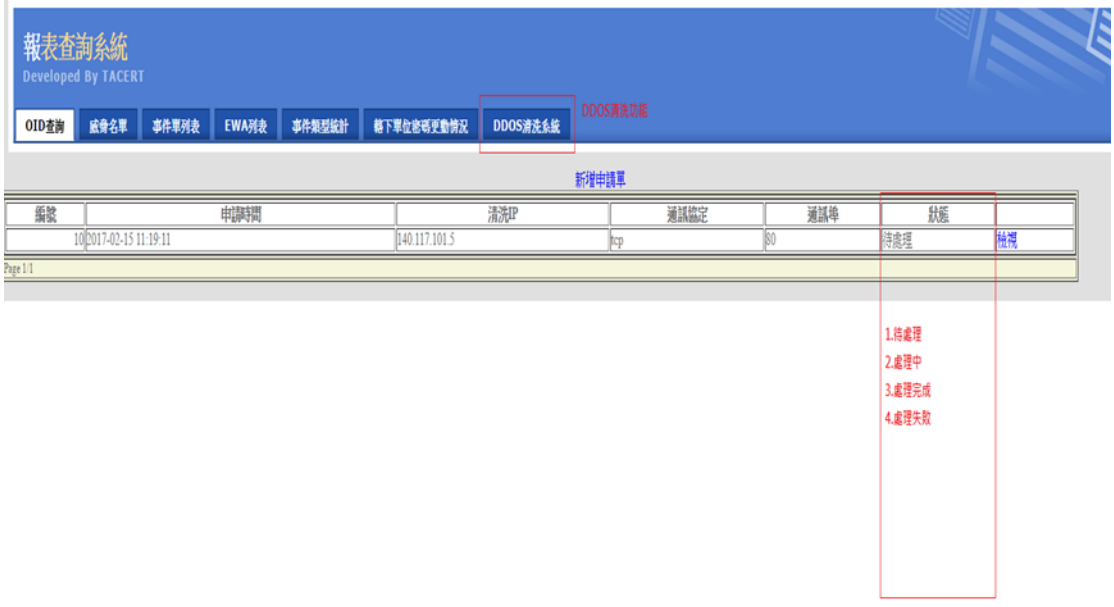


圖 7 檢視 DDoS 工單資訊

② 點選「檢視」即可查詢該工單，如圖 8 所示，其中「回覆意見」為 SOC 對於該 DDOS 工單的回覆(例如:無法清洗的原因)。

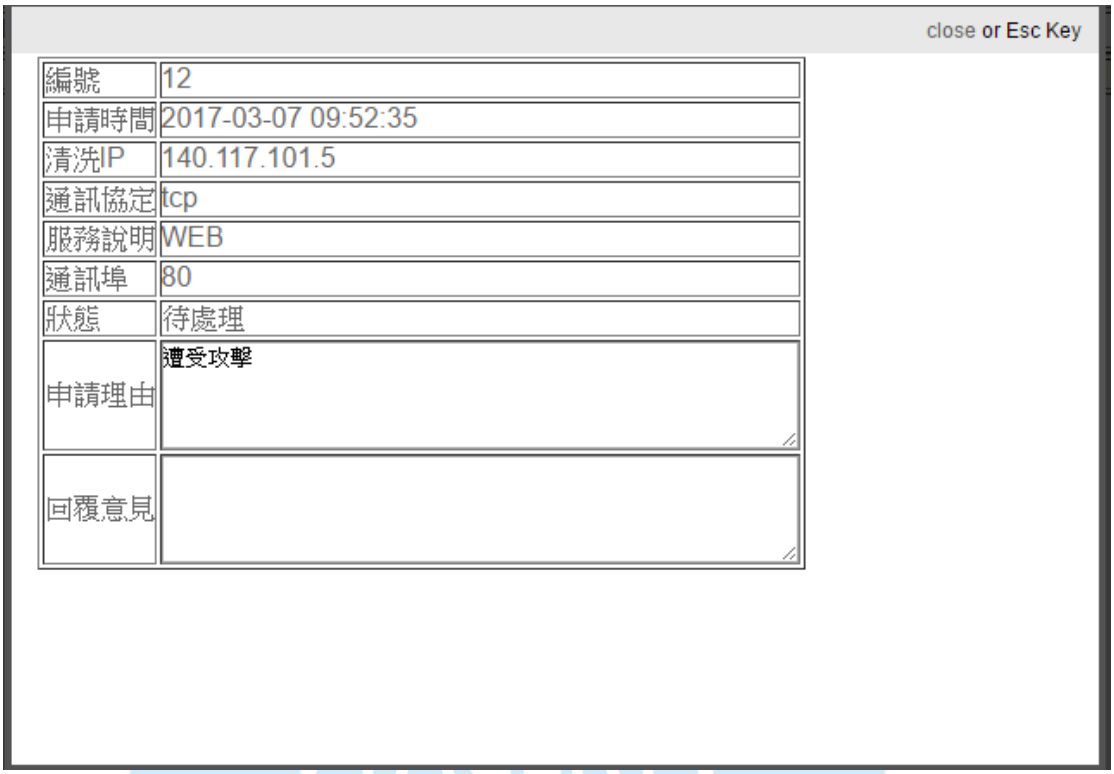


圖 8

**(4) 自動產生告知通報事件單**

當 SOC 中心完成清洗後，會登入 DDoS 清洗系統將工單狀態改為「處理完成」，此時平台會自動產生一張告知通報事件單至「教育機構資安通報應變平台」，連線單位需依照「教育機構資安通報應變流程」完成填寫通報應變->二線區縣市網路中心通報審核->TACERT 團隊通報審核，此 DDoS 攻擊事件單才算完整結案。

## 四、 操作說明(SOC 人員)

### (1) 系統網址及登入說明

①系統網址：https://portal.cert.tanet.edu.tw

選擇「**教育機構資安通報回饋平台**」，如圖 9。


圖 9 教育機構資安通報回饋平台界面

② 於登錄畫面鍵入帳號、密碼及驗證碼，如圖 10。


圖 10 登錄界面

### (2) 新增 DDoS 清洗服務申請

①登入「資安通報回饋系統平台」後先點選上方工作列「DDOS 清洗系統」，再點選「新建 DDOS 工單」。

圖 11 教育機構資安通報回饋平台登錄後的界面

②產生如圖 12 所示的表單，單位名稱可輸入關鍵字，平台會進行模糊比對，再點選出正確的單位名稱，使用者將相關資訊(*為必填欄位)填入，，送出即可。


圖 12 DDOS 清洗申請單表單內容

**(3) 管理 DDoS 工單**

① 點選「管理 DDOS 工單」可查詢到所有 DDoS 工單的狀態。

圖 13 管理 DDOS 工單的界面

②SOC 人員於清洗完成後，可點選「修改」，更改「狀態」以及填寫「回覆理由」。


圖 10