教育機構資安通報平台

資安通報報表系統操作手冊 v2

TACERT 臺灣學術網路危機處理中心團隊 製

2018/5

目錄

一、前言

教育機構資安通報平台自 99 年啟用，資安事件單之數量亦逐年增加。TACERT 營運時得知管理單位對於事件單之追蹤及統計之需要，因此於 101 年度開發「教育機構資安通報平台報表系統(以下簡稱資安通報報表系統)」，系統網址：https://portal.cert.tanet.edu.tw，以利管理單位進行追蹤及統計使用。

二、系統說明

101 年度 TACERT 開發「教育機構資安通報平台報表系統(以下簡稱資安通報報表系統)」，提供二線區縣市網管理人員使用，已完成開發「單位 OID 查詢」、「惡意網站威脅來源清單公告」、「資安事件報表系統」、「資安預警事件報表系統」與「資安攻擊類型趨勢統計」等子系統。106 年陸續新增「轄下單位密碼更動情況系統」及「DDoS 清洗服務申請系統」。

資安通報報表系統功能表如圖 1 所示，系統功能說明如表 1 所示。

圖 1 資安通報報表系統功能表

功能	使用人員	功能說明
A1 單位 OID 暨聯絡人查詢系統	二線人員	區縣市網路中心管理人員與 TACERT 營運團隊可以查詢單位於通報平台內更新的資安連絡人連絡資訊與單位 OID 資訊
A2 惡意網站清單公告系統	二線人員	區縣市網路管理人員可以於此處瀏覽與下載「惡意網站威脅來源清單」的公告資訊。 TACERT 營運團隊每週匯整由各個資安偵測團隊所偵測的「惡意網站威脅來源清單」，並每週定期更新「惡意網站威脅來源清單」。 *107 年 5 月新增「下載技服威脅清單」功能，可個別下載由「行政院國家資通安全會報技術服務中心」所提供的完整惡意網站威脅來源清單。
A3 資安事件單報表系統	二線人員	各區縣市網路中心管理人員或 TACERT 管理人員可於此處利用「單位名稱」或「日期區間」，快速查詢與下載其轄下連線單位的資安事件報表資料，以利進行統計與進行更進一步之追蹤。
A4 資安預警單報表系統	二線人員	各區縣市網路中心管理人員或 TACERT 管理人員可於此處利用「單位名稱」或「日期區間」，快速查詢與下載其轄下連線單位的資安預警事件報表資料，以利進行統計與進行更進一步之追蹤。
A5 資安事件類型統計系統	二線人員	提供所有學術網路資安事件攻擊事件量、事件類型統計報表，讓使用者可了解目前的資安事件攻擊趨勢，進而加以防範。
A6 轄下單位密碼更動情況	二線人員	提供各區縣市網路中心管理人員查詢轄下單位密碼更新狀況，以利追蹤轄下單位是否有確實完成每年度密碼更新作業。
A7 DDoS 清洗系統	二線人員	提供二線區縣市網路中心管理人員協助轄下連線單位申請「DDoS 清洗服務」使用，以及查詢其清洗流程。

表 1 資安通報報表系統功能說明

三、操作說明

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：

STEP 1.

系統網址：https://portal.cert.tanet.edu.tw

選擇「**資安通報報表系統**」，如圖 2。

圖 2

STEP 2.

於登畫面鍵入審核用帳號、密碼(英文+OID 帳號，如 Z2.16…..)及驗證碼，如圖 3。

圖 3

STEP 3.

介面說明：

A. 登入後於上方右側顯示登入帳號及「**登出**」功能，如圖 4 中① 所示。

B. 中央上方顯示子功能頁籤，點選可開啟對應子功能，如圖 4 中②所示。

圖 4

(2) OID 查詢(單位 OID 暨聯絡人查詢系統)

STEP 1.

選擇「**OID 查詢**」開啟單位 OID 暨聯絡人查詢系統，如圖 5。

圖 5

STEP 2.

A. 開啟單位 OID 暨聯絡人查詢系統後，將列出貴單位轄下所有單位及單位連絡人資料，如圖 6 中① 所示。

B. 左上方可針對單位 OID 及名稱進行搜尋動作，輸入進行搜尋的 OID 及名稱後，點選「**送出**」(因瀏覽器定義不同，請勿以 Enter 查詢)，如圖 6 中② 所示。

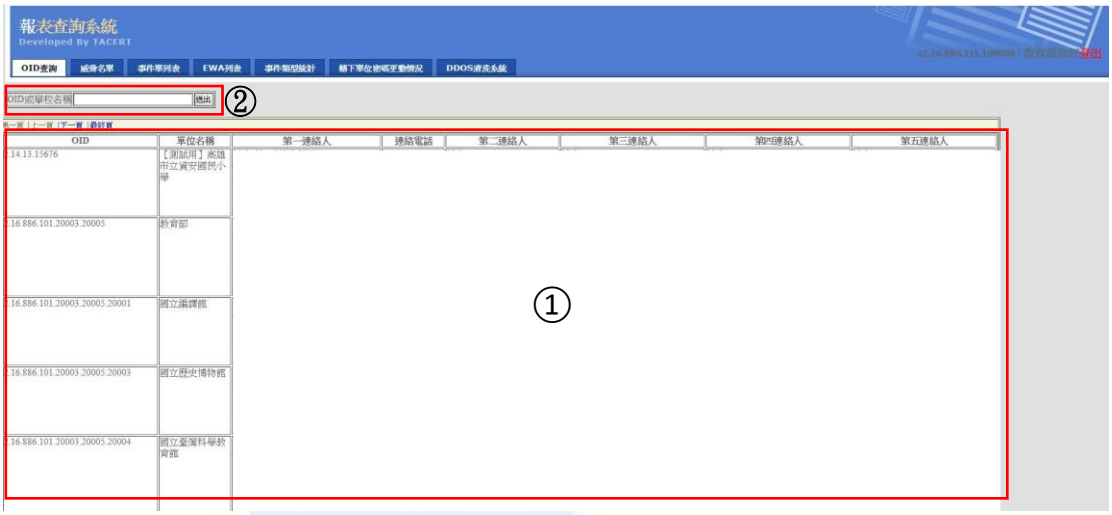

圖 6

(3) 威脅名單(惡意網站威脅來源清單公告系統)

STEP 1.

選擇「**威脅名單**」開啟惡意網站威脅來源清單公告系統，如圖 7。

公告來源	發現日期	IP	惡意網址	攻擊類型	國家
S-ASOC	2018-05-12			網路攻擊	Hong Kong
S-ASOC	2018-05-12			網路攻擊	Ukraine
S-ASOC	2018-05-12			網路攻擊	China
S-ASOC	2018-05-12			網路攻擊	United States
S-ASOC	2018-05-12			網路攻擊	Poland
S-ASOC	2018-05-11			網路攻擊	China
S-ASOC	2018-05-11			網路攻擊	China
S-ASOC	2018-05-11			網路攻擊	Belarus
S-ASOC	2018-05-11			網路攻擊	Venezuela
S-ASOC	2018-05-11			網路攻擊	Venezuela
S-ASOC	2018-05-11			網路攻擊	Macedonia
S-ASOC	2018-05-11			網路攻擊	Netherlands
S-ASOC	2018-05-11			網路攻擊	Netherlands

圖 7

STEP 2.

A. 開啟惡意網站威脅來源清單公告系統後，將列出最新一次更新之威脅名單列表，如圖 8 中① 所示，目前表列近三個月資訊，且固定於每星期三更新。

B. 中央上方可針對表格內欄位進行搜尋動作，輸入進行搜尋之內容後，點選「**Show**」，如圖 8 中② 所示。

C. 如需下載該威脅名單，點選「**下載 TANet 威脅清單**」即可取得最近三個月的完整惡意威脅名單，如圖 9 中①所示；如需個別下載技服中心提供的所有惡意威脅清單，點選「**下載技服威脅清單**」即可取

得，如圖 9 中②所示。

D. 威脅清單內容為機敏性資料，故下載清單會出現「威脅清單內容為機敏性資料，僅供公務使用，嚴禁外流並依公務密件相關規定處理！」的提示視窗，提醒使用者留意，點選「確定」即可下載該清單。

圖 8

圖 9

(4) 事件單列表(資安事件報表系統)

STEP 1.

選擇「**事件單列表**」開啟資安事件報表系統，如圖 10。

圖 10

STEP 2.

A. 開啟資安事件報表系統後，將列出貴單位轄下管理之事件單列表，如圖 11 中① 所示。

B. 中央上方可針對單位、狀態及時間等條件進行搜尋，完成條件輸入後，點選「**顯示**」，如圖 11 中② 所示。

C. 如需匯出報表，完成修件輸入後，點選「**匯出報表**」後點選「**下載 excel 結果**」即可取報表，如圖 12 中①②所示。

圖 11

圖 12

(5) EWA 列表(資安預警事件報表系統)

STEP 1.

選擇「**EWA 列表**」開啟資安預警事件報表系統，如圖 13。

圖 13

STEP 2.

A. 開啟資安預警事件報表系統後，將列出貴單位轄下管理之預警事件單列表，如圖 14 中① 所示。

B. 中央上方可針對單位、狀態及時間等條件進行搜尋，完成條件輸入後，點選「**顯示**」，如圖 14 中② 所示。

C. 如需匯出報表，完成條件輸入後，點選「**匯出報表**」後點選「**下載 excel 結果**」即可取報表，如圖 15 中①②所示。

圖 14

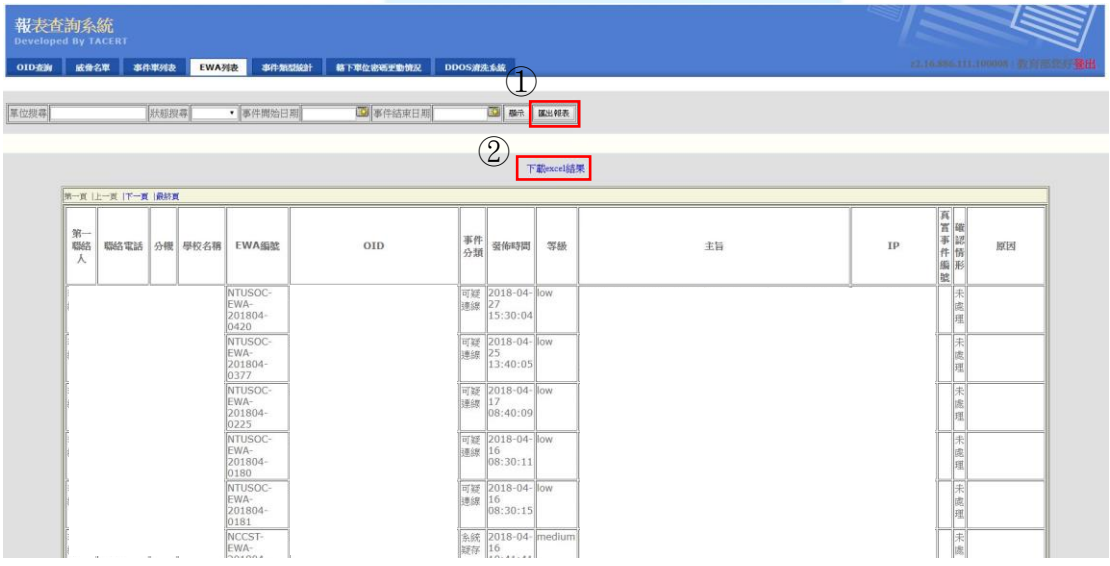

圖 15

(6) 事件類型統計(資安攻擊類型趨勢統計系統)

STEP 1.

選擇「**事件類型統計**」開啟資安攻擊類型趨勢統計系統，如圖 16。

圖 16

STEP 2.

A. 開啟資安攻擊類型趨勢統計系統後，將列出貴單位轄下單位已結案之事件統計資料，如圖 17 中① 所示。且統計出目前貴單位平均審核統計，以供貴單位參考，如圖 17 中②所示。

B. 中央上方可針對單位及時間等條件進行搜尋，完成條件輸入後，點選「**顯示**」，如圖 17 中③所示。

圖 17

(7) 轄下單位密碼更動情況

選擇「**轄下單位密碼更動情況**」開啟轄下單位密碼更新狀況系統，將顯示出所有轄下單位的連絡人密碼更新狀況，如圖 18。

圖 18

(8) DDoS 清洗系統(DDoS 清洗服務申請系統)

STEP 1.

A.選擇「**DDoS 清洗系統**」開啟 DDoS 清洗服務申請系統，如圖 19 中①所示。

B.若要申請 DDoS 清洗服務，點選「新增申請單」，如圖 19 中②所示。

圖 19

STEP 2.

點選「新增申請單」後，系統產生如圖 20 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 20 DDOS 清洗申請單表單內容

STEP 3.檢視 DDoS 工單資訊

A. 點選「DDOS 清洗系統」功能將顯示所有 DDOS 工單資訊，如圖 21 所示，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(已處理完成)
失敗(SOC 處理該工單失敗, 無法清洗)

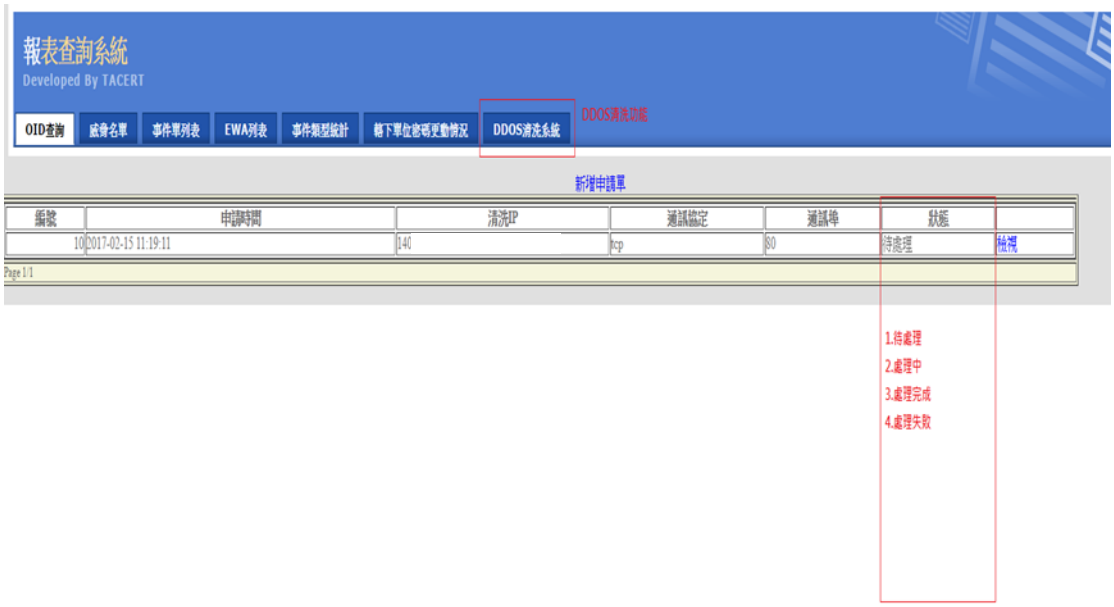

圖 21 檢視 DDoS 工單資訊

B. 點選「檢視」即可查詢該工單，如圖 22 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 22

STEP 4.教育機構資安通報平台自動產行「自行通報」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自行通報事件單(如圖 23 所示)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。

詳細資料			
發佈編號	TANET-DDOS-2018491673	發佈時間	2018-04-09 16:10:29
事件類型	其它類型的入侵攻擊	發現時間	2018-04-09 16:07:03
事件主旨	貴單位遭受外部DDOS攻擊		
事件描述	貴單位所申請的DDOS清洗服務已完成清洗		
手法研判	無		
處理建議		建議貴單位觀察是否仍持續受到DDOS攻擊的影響,請點選INT事件類型中的其它,並輸入DDOS字樣	
參考資料			

1. 通報型態：	自行通報
告知通報編號：	TANET-DDOS-2018491673
2. 事件發生時間：	2018-04-09 16:07:03
3. 設備資料：	
ＩＰ位置：	
網際網路位置：	
設備廠牌、機型：	
作業系統：	
受駭應用軟體：	
已裝置之安全防護軟體：	
	防毒軟體： 防火牆：

圖 23