

## 資安通報平台新增資安事件分類說明

隨著資安事件類型的多樣化，資安通報平台事件分類除了原有的「INT(入侵攻擊)」以及「DEF(網頁攻擊)」以外，新增OTHER(其它事件)類別，其事件類型包含：「設備故障/毀損」、「電力異常」、「網路服務中斷」、「設備遺失」等，事件分類功能截圖如圖 1 所示，以便能更貼切實際之資安事件類型。

◎事件分類：

INT ( 入侵攻擊 ) :

- 系統被入侵(資訊設備遭惡意使用者入侵)
- 對外攻擊(對外部主機進行攻擊行為)
- 針對性攻擊(針對特定個人的資訊洩漏與身分盜取)
- 散播惡意程式(主機對外進行惡意程式散播)
- 中繼站(主機成駭客之中繼站，接收惡意程式連線)
- 電子郵件社交工程攻擊(帳號遭盜用對外發動社交工程攻擊)
- 垃圾郵件(Spam)(資訊設備從事Spam Mail散播行為)
- 命令與控制伺服器(C&C)(主機疑似為駭客之Botnet C&C Server)
- 殭屍電腦(Bot)(資訊設備疑似成為駭客所控制之Botnet成員)
- 其它類型的入侵攻擊

DEF ( 網頁攻擊 ) :

- 惡意網頁(網頁遭駭客置換或放置不當內容)
- 惡意留言(網頁遭駭客放上惡意留言)
- 網頁置換(網頁遭駭客置換)
- 釣魚網頁(主機遭駭客置入釣魚網頁)
- 個資外洩(主機遭個資外洩)
- 其它類型的網頁攻擊

OTHER(其它事件) :

- 設備故障/毀損
- 電力異常
- 網路服務中斷
- 設備遺失
- 其它類型攻擊

圖 1 · 事件分類新增 OTHER(其它事件)類型截圖