

資安通報平台新增資安事件通報事項說明

為能更明確了解資安事件發生狀態並與資安標準接軌，教育機構資安通報平台(<https://info.cert.tanet.edu.tw/>) 將於通報應變作業中新增說明欄位資料，新增欄位預計於 112 年 6 月初正式上線。

一、通報流程新增「受駭設備類型」、「受害設備說明」、「損害類別說明」、「攻擊手法」、「調查說明」、「情資類型」欄位資料，如圖 1 所示，新增欄位說明如下列：

受駭設備類型：	個人電腦
受害設備說明：	<input type="text"/> 範例：同仁桌機
損害類別說明：	資料外洩
攻擊手法：	社交工程
調查說明：	<input type="text"/> 範例：同仁誤執行惡意程式
情資類型：	惡意內容

圖 1.通報流程新增的欄位資料

- 1、「受駭設備類型」：受駭設備類型的欄位選項如圖 2 所示，請就受害之設備選擇適當之對應類型。

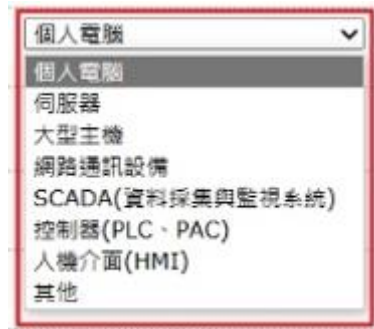


圖 2. 受駭設備類型的欄位選項

- 2、 「受害設備說明」：請簡略說明此設備之用途。
- 3、 「損害類別說明」：選項分為「資料外洩」、「資料竄改」、「硬體損害」、「金錢損失」與「其他」，請依實際狀況選擇適當的損害類型。
- 4、 「攻擊手法」：攻擊手法的欄位選項如圖 3 所示，請選擇攻擊者所使用的攻擊手法類型。



圖 3. 攻擊手法的欄位選項

- 5、 「調查說明」：請簡略的說明，相關事件的調查結果。

6、「情資類型」：此資訊為事件原始情資來源之資訊類型，共可分為下列 10 項類型，請選擇適當之類型。

- (1). 惡意內容：針對透過文字、照片、影片等形式散播不當內容之事件。
- (2). 惡意程式：針對與相關惡意程式之事件。
- (3). 資訊蒐集：針對透過掃描、探測及社交工程等攻擊手法取得資訊之事件。
- (4). 入侵嘗試：針對嘗試入侵未經授權主機之事件。
- (5). 入侵攻擊：針對系統遭未經授權存取或取得系統/使用者權限之事件。
- (6). 阻斷服務：針對影響服務可用性或造成服務中斷之攻擊事件。
- (7). 資訊內容安全：針對系統遭未經驗證存取或影響資訊機敏性之事件。
- (8). 詐欺攻擊：針對偽冒他人身分、系統服務及組織等進行攻擊行為之事件。
- (9). 系統弱點：針對系統存在弱點之事件。
- (10). 其他：非屬前述資安事件類型之事件資訊。

二、 應變流程新增「損害控管狀態」的欄位資料，如圖 4 所示。

應變流程

1. 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

2. 解決辦法：
(文字勿超過200中文字)

3. 完成損害控制時間：
2023-05-29 10:37:23

4. 損害控制狀態：
是：完成損害控制
是：完成損害控制
是：完成損害控制與復原

圖 4.應變流程新增的欄位資料

「損害控制狀態」可分為完成下列兩種狀態，請依實際狀況選擇適合的選項：

- 1、 損害控制：已控管此事件所造成的危害。
- 2、 完成損害控制與復原：已控管此事件所造成的危害並已完成系統復原。