資安通報與服務

游忠憲

國立臺灣大學

NTU
National Taiwan University

大綱

- 教育部資安通報流程
- 弱點監測掃描平台
- 防洩漏個資掃描平台
- IPS異常報告

教育部資安通報流程

- 範例說明：

發佈編號	NTUSOC-INT-201302-XXXX	**發佈時間**	2013-02-XX 12:57:49
事件類型	系統被入侵	**發現時間**	2013-02-XX 15:23:00
事件主旨	教育部資安事件通告－OO 國民小學[XXX.XXX.XXX.XXX]主機疑似中毒警訊通知		
事件描述	本中心研判來源主機疑似感染病毒，並對目標主機進行可疑連線。請針對該來源 IP 執行程式內容與系統安全狀態檢測，並恢復系統正常運作狀態，來降低受駭範圍。 入侵偵測系統偵測到使用者主機 (XXX.XXX.XXX.XXX) 可能感染電腦病毒，嘗試傳送惡意封包攻擊目標 IP（多個目標 IP）。		
手法研判	無		
處理建議	更新防毒軟體的病毒碼或安裝相關修正檔，或關閉不使用的應用軟體與通信埠以及定期執行弱點掃描程式。 利用資安網站所提供的自動檢查及移除程式來檢查電腦所感染到的蠕蟲病毒。 建議用戶收到未經授權的來源 IP 存取，可在防火牆上阻擋外部 IP 來存取主機。 請用戶留意主機有無異常動作。(如：新增帳號、開啟不明 Port、或執行不明程式) 若目標 IP 用戶皆無上述問題，則請用戶多注意來源 IP 將可能發動攻擊。 時常查閱網路上著名資安網站所公佈相關訊息。		
參考資料	無		

教育部資安通報流程(cont.)

- 範例說明(cont.)：

各機關因受外在因素所產生資通安全事件時通報事項：

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：「;」、「"」、「'」、「$」、「&」、「%」、「!」、「^」、「*」、「<」、「>」、「_」、「|」、「-」

1. 通報型態: ■告知通報

2. 事件發生時間：

◎IP 位置（IP address）：
範例: 120.114.2

此欄位填入被通報之 IP

◎網際網路位置（web-url）：
範例: https://www.xxx.edu.tw/cba.index

教育部資安通報流程(cont.)

- 範例說明(cont.)：

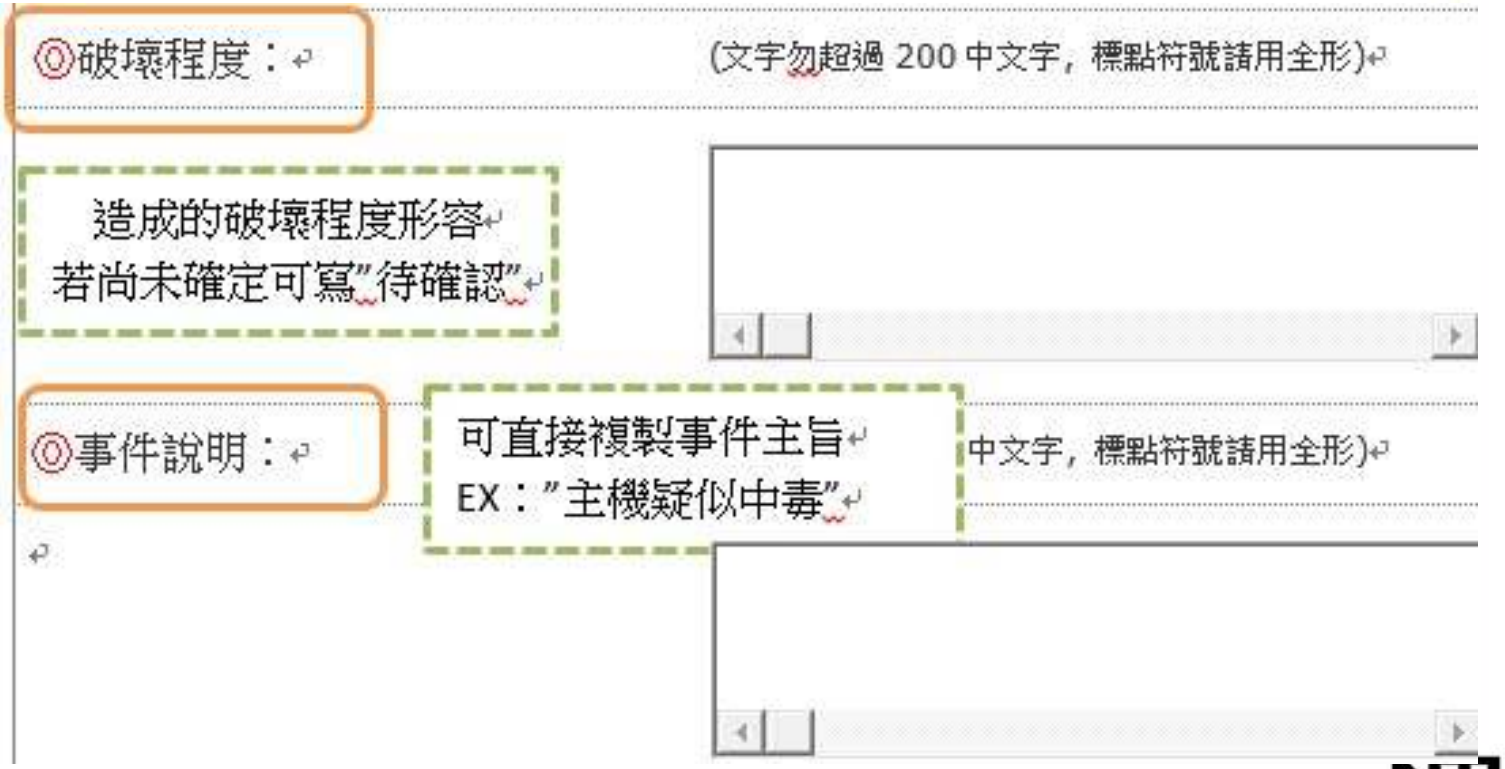
◎作業系統（名稱/版本）：	此欄位填入該主機作業系統 若尚無法得知可寫"待確認" 範例 1:Centos Linux 5. 範例 2: Windows XP SP2
◎受駭應用軟體（名稱/版本）：	範例: sendmail server，此為不確定版本的範例
◎已裝置之安全防護軟體:	
防毒軟體（名稱/版本):	範例: Avira 10.0.0.561

教育部資安通報流程(cont.)

- 範例說明(cont.)：

教育部資安通報流程(cont.)

- 範例說明(cont.)：



教育部資安通報流程(cont.)

- 範例說明(cont.)：

5. 資通安全事件：影響等級及說明

1. 事件等級：取底下三個欄位中最高等級當成最後之事件等級
2. 第 3、4 級事件係屬於重大資安事件，教育部各長官需親自督導進度
3. 若有 3、4 級事件，請立刻電話告知您所屬的主管機關
4. 如果您無法確定如何填寫時，請電話連絡您所屬的主管機關請求協助
5. 等級 0 之資安事件教育部另有規範，請至少填入等級 1

◎資安事件判斷：　若無特別事件皆為一級事件

(1) 機密性衝擊 -

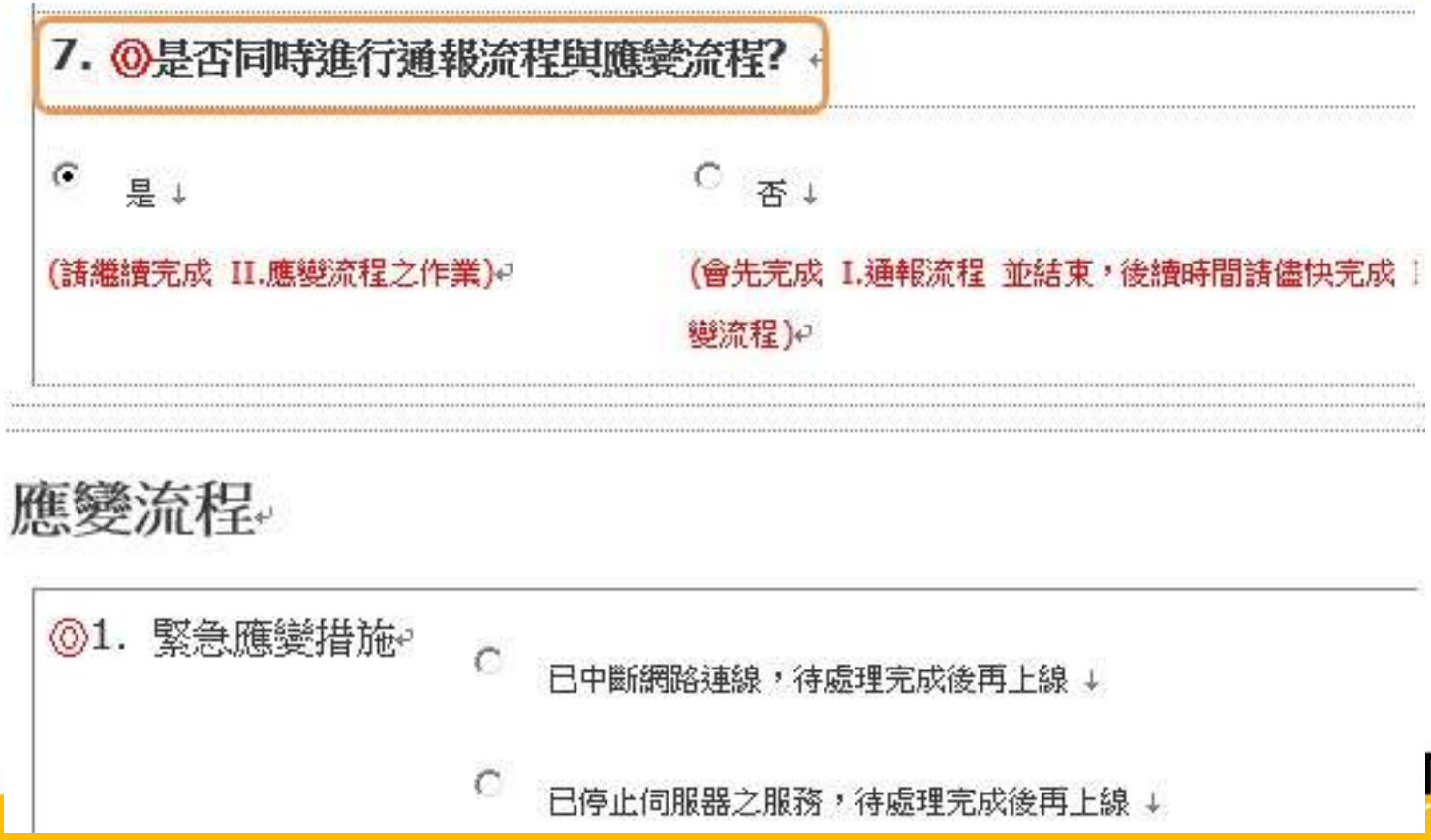
1 級-非核心業務資料遭洩漏

教育部資安通報流程(cont.)

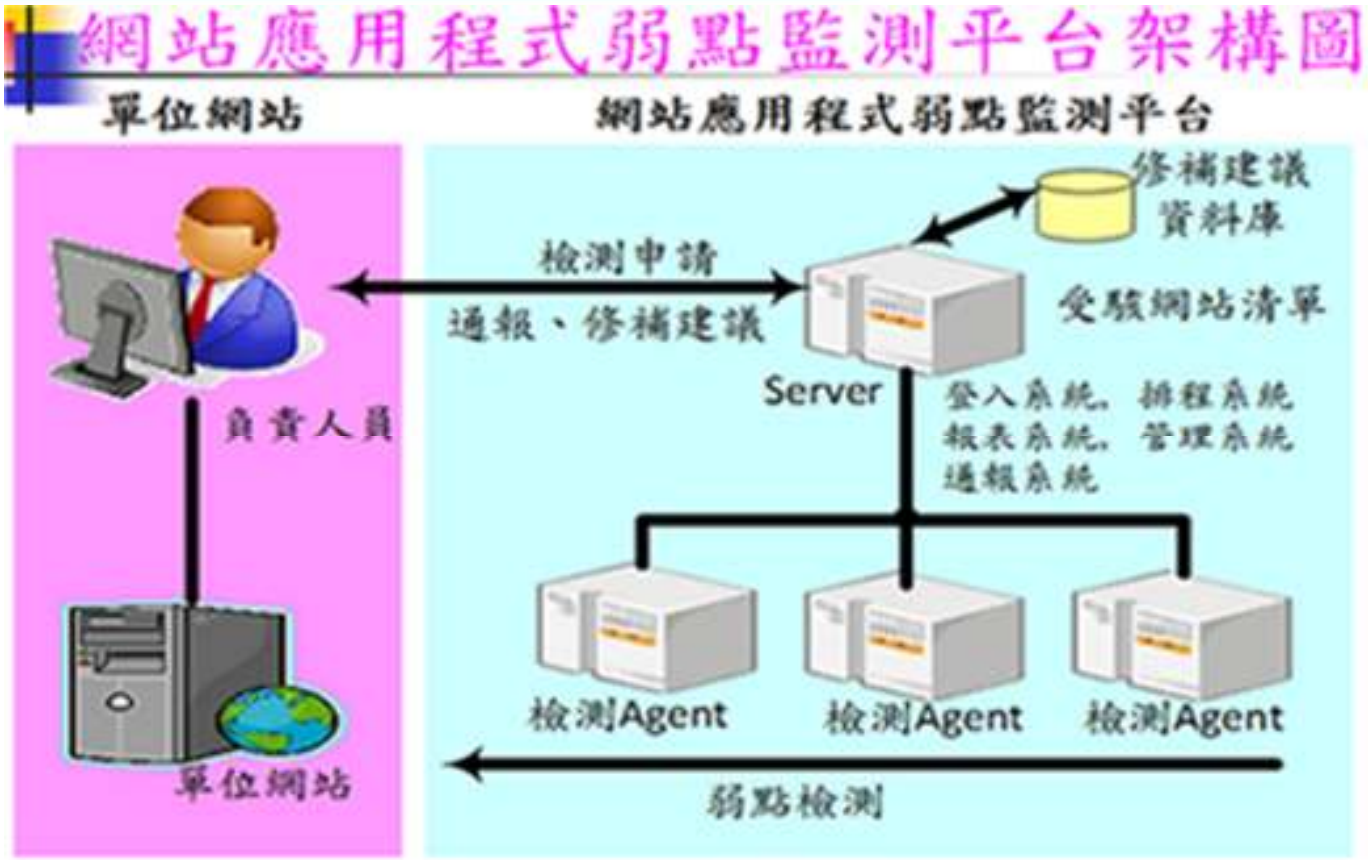
- 範例說明(cont.)：

教育部資安通報流程(cont.)

- 範例說明(cont.)：



弱點監測平台架構圖


網站應用程式弱點監測平台架構圖
單位網站
網站應用程式弱點監測平台
修補建議
資料庫
檢測申請
通報、修補建議
受駭網站清單
Server
登入系統、排程系統
報表系統、管理系統
通報系統
負責人員
檢測Agent
檢測Agent
檢測Agent
單位網站
弱點檢測

國立臺灣大學

弱點監測平台特色

弱點監測平台特色(cont.)

國立臺灣大學

NTU
National Taiwan University

防洩漏個資掃瞄平台簡介

- 協助教育單位評估可能洩漏個資的風險
- 針對網站開放性區域
- 提供個資洩漏風險分析報告

國立臺灣大學

NTU
National Taiwan University

防洩漏個資掃瞄平台特色

國立臺灣大學

NTU
National Taiwan University

防洩漏個資掃瞄平台特色(cont.)

國立臺灣大學

NTU
National Taiwan University

入侵防護系統異常報告

- 03/19有部分學校通報瀏覽web發生異常，如：YAHOO、蘋果日報、udn新聞網等。
- 進入IPS檢視後，並未發現有任何異常狀況或巨量事件。
- 將IPS bypass測試後，瀏覽web恢復正常。
- 當天下午約2:00將IPS inline測試，於半小時後再次發生異常，隨即切換bypass。
- IPS原廠隨後遠端進入處理，並於下班時間(17:30~18:30)測試並無異常。
- 公告於03/24上班時間(09:00~12:00)測試，除了偶爾會出現異常狀況，並無法重現03/19的災情。
- 目前原廠人員已將資料交給後線分析，於分析報告出來時會於區網網站公布。