



國立臺灣大學

資安通報與服務

游忠憲



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：120.114.23

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)：	<input type="text"/>	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)：	<input type="text"/>	
範例: <u>sendmail</u> server, 此為不確定版本的範例		
◎已裝置之安全防護軟體：	<input type="text"/>	
防毒軟體 (名稱/版本)：	<input type="text"/>	
範例: Avira 10.0.0.561		



教育部資安通報流程(cont.)

- 範例說明(cont.)：

其它 (名稱/版本):

4. 資通安全事件：基本資料

◎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) ↓



教育部資安通報流程(cont.)

- 範例說明(cont.)：

◎破壞程度：

(文字勿超過 200 中文字，標點符號請用全形)

造成的破壞程度形容
若尚未確定可寫“待確認”

◎事件說明：

可直接複製事件主旨
EX：“主機疑似中毒”

中文字，標點符號請用全形)



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.)：

◎可能影響範圍及損失評估

(文字勿超過 200 字，標點符號請用全形)

若尚無法評估可寫“待評估”



教育部資安通報流程(cont.)

- 範例說明(cont.)：

7. ⑦是否同時進行通報流程與應變流程？

☒ 是 ↓

(請繼續完成 II.應變流程之作業)

☐ 否 ↓

(會先完成 I.通報流程 並結束，後續時間請儘快完成
變流程)

應變流程

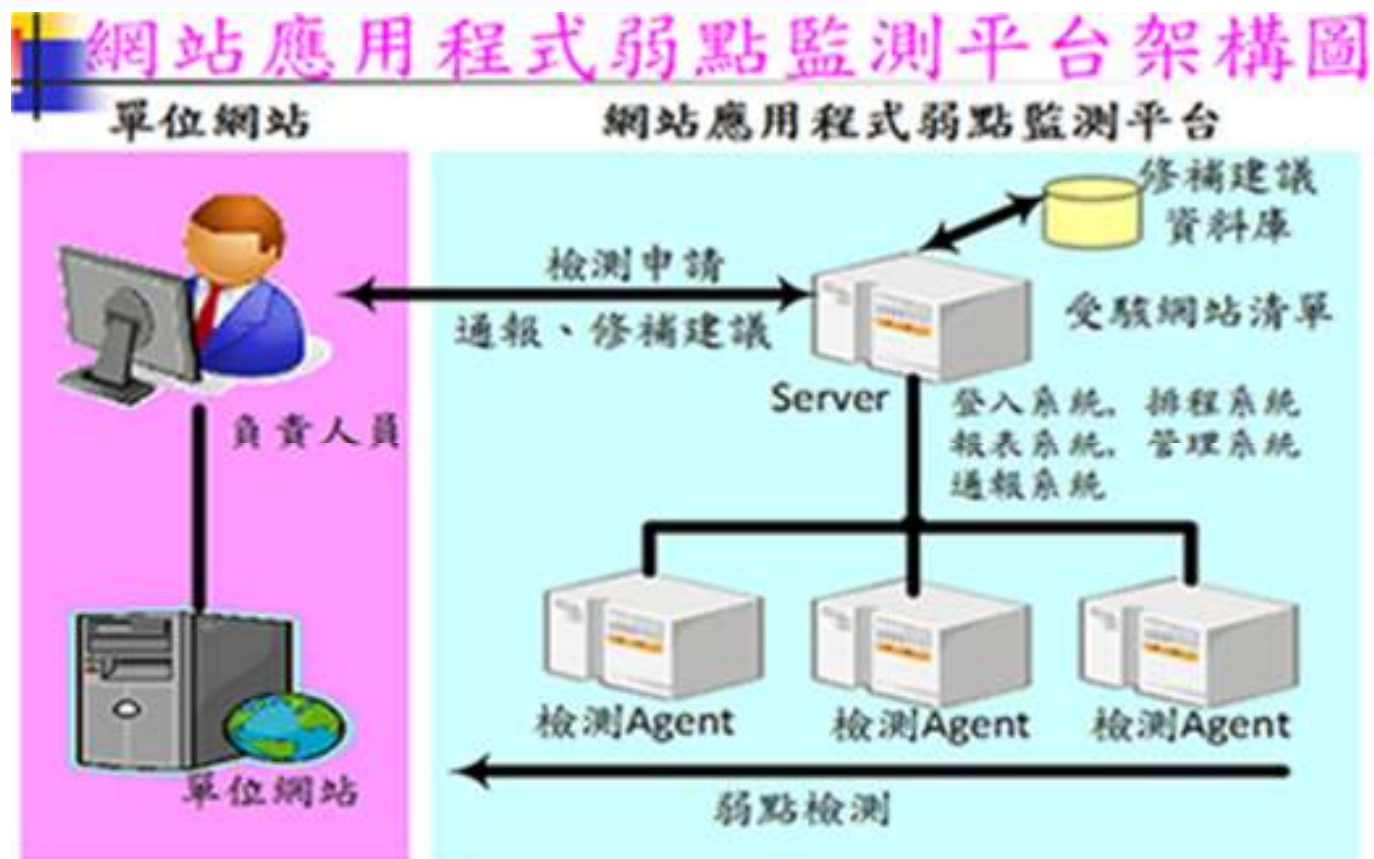
①1. 緊急應變措施

☐ 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 ↓



弱點監測平台架構圖





弱點監測平台特色

最新消息

關於系統

下載專區

問 & 答

網站維護

網站排程

網站結果

修補建議查詢

列印檢測同意書

重建與重打

退出程序

目前位置：網站排程

• 最近設定排程時間：2010/11/9 下午 05:25:19

• 排程間隔時間：0 小時

• 同時線上可排程數：10

• 目前線上排程數：0 (包含等待中、執行中、經過處理中)

• 剩餘可排程數：10

• 剩餘可排程數：10

網站排程

檢測網址：

☒ XSS檢測 [不使用POST檢測]

☒ SQL Injection檢測 [不使用POST檢測]

☒ 惡意檔案執行檢測

☒ 子彈當配置處理檢測

☒ 目錄索引檢測

☒ 傳佈檔案檢測

排程選擇：

檢測時間特規：☒ 輪流時段
日間 (06:00~18:00)
夜間 (18:00~06:00)

保存與重登入設定 幫助

設定已中斷排程

檢測網址：

排程選擇：

檢測時間特規：☒ 輪流時段
日間 (06:00~18:00)
夜間 (18:00~06:00)

取消排程

檢測網址：

相關產品

網站排程

網站排程

網站排程

網站排程

2010年11月

日	一	二	三	四	五	六
	1 請排 請排	2 請排 請排	3 請排 請排	4 請排 請排	5 請排 請排	6 請排 請排
7 請排 請排	8 請排 請排	9 請排 請排	10 請排 請排	11 請排 請排	12 請排 請排	13 請排 請排
14 請排 請排	15 請排 請排	16 請排 請排	17 請排 請排	18 請排 請排	19 請排 請排	20 請排 請排
21 請排 請排	22 請排 請排	23 請排 請排	24 請排 請排	25 請排 請排	26 請排 請排	27 請排 請排
28 請排 請排	29 請排 請排	30 請排 請排				

*檢測時間說明：

1. 日間：每日早上06:00~每日18:00

2. 夜間：每日下午18:00~隔日06:00



弱點監測平台特色(cont.)





防洩漏個資掃描平台簡介

- 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



防洩漏個資掃描平台特色

檢測關鍵字

系統資訊

1. 關鍵字區分自定與系統預設，使用者可自定關鍵字加強檢測結果。

自訂

自訂	建立時間	功能
系統預設		
清單	2011-07-23	<input type="button" value=""/>
身份證字號	2011-05-16	<input type="button" value=""/>
行動電話	2011-05-16	<input type="button" value=""/>
關鍵字	2011-05-06	<input type="button" value=""/>

第一頁 上一頁 1 下一頁 最後一頁 1/1



防洩漏個資掃描平台特色(cont.)





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。