資通安全事件通報單

政府機關(構)應至國家資通安全通報應變網站（http://www.ncert.nat.gov.tw）通報資安事件，若因故無法上網填報，可先填具本通報單以傳真或郵寄方式傳送至國家資通安全會報政府資通安全組，惟待網路連線恢復後仍需上網補登通報。

傳真專線：(02)27331655　　郵寄地址：台北市大安區 106 富陽街 116 號

諮詢專線：(02)27339922

注意事項

1.「◎」為必填項目。

2.請依通報之資安「事件分類」填寫通報單，並依事件類別回傳通報單內容。

3.事件通報的部分請回傳 P1-P3，事件通報並結案的部分請根據事件分類回傳對應的頁碼(網頁攻擊 P1-P7、非法入侵 P1-P3,P8-P10、阻斷服務 P1-P3,P11-P12、設備異常 P1-P3,P13-P14、其他 P1-P3,P15-P17)

◎填報時間：____年____月____日____時____分

STEP1.請填寫事件相關基本資料

一、發生資通安全事件之機關(機構)聯絡資料：

◎機關(機構)名稱：_____◎主管機關名稱：_____

◎通報人：_____　◎電話：_____　傳真：_____

◎電子郵件信箱：_____

◎是否代其他機關(構)通報：□是，該單位名稱_____　□否

◎資安監控中心(SOC)：□無　□機關自行建置

□委外建置，該廠商名稱_____

◎資安維護廠商：_____

STEP2.請詳述事件發生過程

二、事件發生過程：

◎事件發生時間：_____年____月____日____時____分

◎事件分類與異常狀況：(事件分類為單選項；異常狀況為複選項)

〇網頁攻擊

□網頁置換 □惡意留言 □惡意網頁 □釣魚網頁

□網頁木馬 □網站個資外洩

〇非法入侵

□系統遭入侵 □植入惡意程式 □異常連線 □發送垃圾郵件

□資料外洩

〇阻斷服務(DoS/DDoS)

□服務中斷 □效能降低

〇設備問題
□設備毀損 □電力異常 □網路服務中斷 □設備遺失

〇其他：_____

◎事件說明及影響範圍：
_____
_____
_____
_____

◎是否影響其他政府機關(構)或重要民生設施運作：□是 □否

◎此事件通報來源：□自行發現 □警訊通知，發布編號：_____

STEP3.評估事件影響等級

三、事件影響等級：

◎請分別評估資安事件造成之機密性、完整性以及可用性衝擊：
資安事件影響等級為機密性、完整性及可用性衝擊最嚴重者(數字最大者)

－機密性衝擊：(單選)
□國家機密資料遭洩漏(4 級)
□密級或敏感公務資料遭洩漏(3 級)
□核心業務(含關鍵資訊基礎設施)一般資料遭洩漏(2 級)
□非核心業務一般資料遭洩漏(1 級)
□無資料遭洩漏(無需通報)

－完整性衝擊：(單選)
□關鍵資訊基礎設施系統或資料遭嚴重竄改(4 級)
□核心業務系統或資料遭嚴重竄改；抑或關鍵資訊基礎設施系統或資料遭輕微竄改(3 級)
□非核心業務系統或資料遭嚴重竄改；抑或核心業務系統或資料遭輕微竄改(2 級)
□非核心業務系統或資料遭竄改(1 級)
□無系統或資料遭竄改(無需通報)

－可用性衝擊：(單選)
□關鍵資訊基礎設施運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作(4 級)
□核心業務運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作；抑或關鍵資訊基礎設施運作遭影響或系統停頓，於可容忍中斷時間內回復正常運作(3 級)
□非核心業務運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作；抑或核心業務運作遭影響或系統停頓，於可容忍中斷時間內回復正常運作(2 級)
□非核心業務運作遭影響或系統停頓，於可容忍中斷時間內回復正常

運作(1 級)

□無系統或設備運作受影響(無需通報)

Step4.評估是否需要外部支援

四、期望支援項目：

◎是否需要支援：

□是（請續填期望支援內容）　　□否（免填期望支援內容）

期望支援內容：(請勿超過 200 字)

_____

_____

_____

_____

Step5.請填寫機關緊急應變措施-網頁攻擊(請回傳 P1-P7)

五、完成損害控制與復原：

◎保留受害期間之相關設備紀錄資料〈複選〉(最少選填一項，如未保留相關紀錄，請於「其他保留資料或資料處置說明」欄位說明)

☐ 已保存遭入侵主機事件紀錄檔〈單選〉
〈☐1 個月　1-6 個月　6 個月以上　其他_____〉

☐ 已保存防火牆紀錄〈單選〉
〈☐1 個月　1-6 個月　6 個月以上　其他_____〉

☐ 已保存網站日誌檔〈單選〉
〈☐1 個月　1-6 個月　6 個月以上　其他_____〉

☐ 已保存未授權存在之惡意網頁/留言/檔案/程式樣本，共_____個

☐ 其他保留資料或資料處置說明【如未保存資料亦請說明】

_____

_____

◎事件分析與影響評估〈複選〉(最少選填一項，如無對應分析評估結果，請於「影響評估說明補充」欄位說明)，經分析已保存之紀錄，是否發現下列異常情形：

☐ 異常連線行為【請列出異常 IP 與異常連線原因，如：存取後台管理頁面】

_____

_____

☐ 異常帳號使用【請列出帳號並說明帳號權限，與判別準則，如：非上班時間帳號異常登入/登出】

_____

_____

☐ 清查網頁目錄內容，網站內存在未授權之程式/檔案【請說明程式名稱或路徑、檔名】

_____

_____

☐ 網站資料庫內容遭竄改

☐ 發現資料外洩情況【如：異常打包資料，請說明外洩資料類型/欄位與筆數，如：個人資料/機密性資料/非機敏性資料】

_____

_____

☐ 影響評估說明補充【請填寫補充說明】

_____

_____

◎封鎖、根除及復原〈複選〉(最少選填一項，如無對應變處理方式，請於

「應變措施補充說明」欄位說明)因應分析結果，執行處置措施：

- ☐ 移除未授權存在之惡意網頁/留言/檔案，共____筆(必填)
  【請說明程式名稱或路徑、檔名，如無須移除，請填寫「無」】
  _____
  _____
- ☐ 將異常外部連線 IP 列入阻擋清單(必填)【請說明設定阻擋之資訊設備與阻擋之 IP，如無須阻擋，請填寫「無」】
  _____
  _____
- ☐ 停用/刪除異常帳號(必填)【請說明停用/刪除之帳號，如無須刪除，請填寫「無」】
  _____
  _____
- ☐ 移除網站外洩資料
- ☐ 通知事件相關當事人，並依內部資安通報作業向上級呈報
- ☐ 暫時中斷受害主機網路連線行為至主機無安全性疑慮
- ☐ 已向搜尋引擎提供者申請移除庫存頁面〈複選〉
  《☐Google☐Yahoo☐Yam(蕃薯藤) ☐Bing☐Hinet
  ☐其他搜尋引擎提供者_____》
- ☐ 修改網站程式碼，並檢視其他網站程式碼，完成日期_____
- ☐ 重新建置作業系統與作業環境，完成日期_____
- ☐ 應變措施補充說明【請填寫補充說明】
  _____
  _____

STEP6.資安事件結案作業-網頁攻擊(請回傳 P1-P7)

六、事件調查與處理：

◎受害資訊設備數量：電腦總計_____臺；伺服器總計_____臺

◎IP 位址(IP Address)(無；可免填)

外部 IP：_____

內部 IP：_____

◎網際網路位址（Web-URL）(無；可免填)：_____

◎作業系統名稱、版本：

□Windows 系列 □Linux 系列 □其他作業平台 版本：_____

◎已裝置之安全機制：

□防火牆 □防毒軟體 □入侵偵測系統 □入侵防禦系統 □其他：_____

◎受害系統是否通過資安管理認證(ISMS)：□是 □否

◎事件發生原因〈單選〉

〈□作業系統漏洞□弱密碼□應用程式漏洞□網站設計不當

□人為疏失□設定錯誤□系統遭入侵□其他_____〉

◎請簡述事件處理情況：_____

_____

_____

◎補強措施〈複選〉

I. 補強系統/程式安全設定

☐ 已完成評估變更透過受害主機登入應用系統密碼之必要性(如：使用受害主機登入之網域帳號密碼、公務系統帳號密碼、郵件帳號密碼等)**(必填)**

☐ 已完成評估變更受害主機中所有帳號之密碼(含本機管理者) **(必填)**

☐ 已完成檢視/更新受害主機系統與所有應用程式至最新版本(包含網站編輯管理程式，如：FrontPage) **(必填)**【請說明主要更新之程式名稱，如無須更新，請填寫「皆已更新至最新版本」】

_____

_____

☐ 關閉網路芳鄰功能

☐ 設定 robots.txt 檔，控制網站可被搜尋頁面

☐ 已針對所有需要特殊存取權限之網頁加強身分驗證機制【請說明機制名稱或類別】

_____

_____

☐ 限制網站主機上傳之附件檔案類型【請說明附檔名】

_____

_____

☐ 限制網頁存取資料庫的使用權限，對於讀取資料庫資料的帳戶身分及權限加以管制

☐ 限制連線資料庫之主機 IP

☐ 關閉 WebDAV(Web Distribution Authoring and Versioning)

II. 資安管理與教育訓練

☐ 重新檢視機關網路架構適切性

☐ 機關內部全面性安全檢測

☐ 加強內部同仁資安教育訓練

☐ 修正內部資安防護計畫

◎其他相關安全處置【請填寫其他安全處置】

_____

_____

◎完成修復時間：_____年_____月____日____時____分

Step5.請填寫機關緊急應變措施-非法入侵(請回傳 P1-P3、P8-P10)

五、完成損害控制與復原：

◎保留受害期間之相關設備紀錄資料〈複選〉(最少選填一項，如未保留相關紀錄，請於「其他保留資料或資料處置說明」欄位說明)

☐ 已保存遭受害主機事件紀錄檔〈單選〉

〈☐1 個月　1-6 個月　6 個月以上　其他_____〉

☐ 已保存防火牆紀錄〈單選〉

〈☐1 個月　1-6 個月　6 個月以上　其他_____〉

☐ 已保存未授權存在之惡意網頁/留言/檔案/程式樣本，共_____個

☐ 其他保留資料或資料處置說明【如未保存資料亦請說明】

_____

_____

◎事件分析與影響評估〈複選〉(最少選填一項，如無對應分析評估結果，請於「影響評估說明補充」欄位說明)經分析已保存之紀錄，是否發現下列異常情形：

☐ 異常連線行為【請列出異常 IP 與異常連線，如：存取後台管理頁面】

_____

_____

☐ 異常帳號使用【請列出帳號並說帳號權限，與判別準則，如：非上班時間帳號異常登入/登出】

_____

_____

☐ 發現資料外洩情況【如：異常打包資料，請說明外洩資料類型/欄位與筆數，如：個人資料/機密性資料/非機敏性資料】

_____

_____

☐ 影響評估補充說明【請填寫補充說明】

_____

_____

◎封鎖、根除及復原〈複選〉(最少選填一項，如無對應變處理方式，請於「應變措施補充說明」欄位說明)因應分析結果，執行處置措施：

☐ 移除未授權存在之惡意網頁/留言/檔案/程式，共_____筆(必填)【請說明程式名稱或路徑、檔名，如無須移除，請填寫「無」】

_____

_____

☐ 將可疑 IP/Domain Name 列入阻擋清單(必填)【請說明設定阻擋之

資訊設備與阻擋之 IP，如無須阻擋，請填寫「無」】

_____

_____

☐ 停用/刪除異常帳號(必填)【請說明停用/刪除之帳號，如無須移除，請填寫「無」】

_____

_____

☐ 中斷受害主機網路連線行為至主機無安全性疑慮

☐ 重新建置作業系統與作業環境，完成日期_____

☐ 惡意程式樣本送交防毒軟體廠商，共____個

☐ 應變措施補充說明【請填寫補充說明】

_____

_____

Step6.資安事件結案作業-非法入侵(請回傳 P1-P3、P8-P10)

六、事件調查與處理：

◎受害資訊設備數量：電腦總計____臺；伺服器總計_____臺

◎IP 位址(IP Address)(無；可免填)

外部 IP：_____

內部 IP：_____

◎網際網路位址（Web-URL）(無；可免填)：_____

◎作業系統名稱、版本：

☐Windows 系列 ☐Linux 系列 ☐其他作業平台 版本：_____

◎已裝置之安全機制：

☐防火牆 ☐防毒軟體 ☐入侵偵測系統 ☐入侵防禦系統 ☐其他：____

◎受害系統是否通過資安管理認證(ISMS)：☐是 ☐否

◎事件發生原因〈單選〉

〈☐社交工程☐作業系統漏洞☐弱密碼☐應用程式漏洞☐網站設計不當 ☐系統遭入侵☐其他_____〉【請說明事件調查情況】

_____

_____

◎補強措施〈複選〉

I. 補強系統/程式安全設定〈複選〉

☐ 已完成評估變更透過受害主機登入應用系統密碼之必要性(如：使用受害主機登入之網域帳號密碼、公務系統帳號密碼、郵件帳號密

碼等) **(必填)**

☐ 已完成評估變更受害主機中所有帳號密碼之必要性(含本機管理者) **(必填)**

☐ 已完成檢視/更新受害主機系統與所有應用程式至最新版本**(必填)**
【請說明主要更新之程式名稱，如無須更新，請填寫「皆已更新至最新版本」】

_____

_____

☐ 關閉郵件伺服器 Open Relay 功能

☐ 關閉網路芳鄰功能

II. 資安管理與教育訓練(複選)

☐ 重新檢視機關網路架構適切性

☐ 機關內部全面性安全檢測

☐ 加強內部同仁資安教育訓練

☐ 修正內部資安防護計畫

◎其他相關安全處置【請填寫其他安全處置】

_____

_____

◎已解決時間：_____年_____月____日____時____分

Step5.請填寫機關緊急應變措施-阻斷服務(DoS/DDoS) (請回傳 P1-P3、P11-P12)

五、完成損害控制與復原：

◎保留受害期間之相關設備紀錄資料〈複選〉(最少選填一項，如未保留相關紀錄，請於「其他保留資料或資料處置說明」欄位說明)

☐ 已保存遭入侵主機事件檢視器〈單選〉

〈☐1 個月　1-6 個月　6 個月以上　其他_____〉

☐ 已保存防火牆紀錄〈單選〉

〈☐1 個月　1-6 個月　6 個月以上　其他_____〉

☐ 已保存受攻擊主機封包紀錄〈☐10 分鐘　10-30 分鐘　30-60 分鐘〉

☐ 其他保留資料或資料處置說明【如未保存資料亦請說明】

_____

_____

◎事件分析與影響評估〈複選〉(最少選填一項，如無對應分析評估結果，請於「影響評估說明補充」欄位說明)

☐ 攻擊來源 IP 數量_____個

☐ 確認遭攻擊主機用途【請說明主機用途】

_____

_____

☐ 影響評估補充說明

_____

_____

◎封鎖、根除及復原〈複選〉(最少選填一項，如無對應變處理方式，請於「應變措施補充說明」欄位說明)

☐ 阻擋攻擊來源 IP(必填)【請說明設定阻擋之資訊設備與阻擋之 IP，如無須阻擋，請填寫「無」】

_____

_____

☐ 調整網路頻寬

☐ 聯繫網路服務提供業者(ISP)_____(請提供 ISP 業者名稱)，請其協助進行阻擋

☐ 應變措施補充說明【請填寫補充說明】

_____

_____

Step6.資安事件結案作業-阻斷服務(DoS/DDoS) (請回傳 P1-P3、P11-P12)

六、事件調查與處理：

◎受害資訊設備數量：電腦總計_____臺；伺服器總計_____臺

◎IP 位址(IP Address)(無；可免填)

外部 IP：_____

內部 IP：_____

◎網際網路位址（Web-URL）(無；可免填)：_____

◎作業系統名稱、版本：

□Windows 系列 □Linux 系列 □其他作業平台 版本：_____

◎已裝置之安全機制：

□防火牆 □防毒軟體 □入侵偵測系統 □入侵防禦系統 □其他：_____

◎受害系統是否通過資安管理認證(ISMS)：□是 □否

◎補強措施〈複選〉

I. 補強系統/程式安全設定〈複選〉

☐ 限制同時間單一 IP 連線

☐ DNS 主機停用外部遞迴查詢

☐ 已完成檢視/移除主機/伺服器不必要服務功能(必填)【請說明服務功能名稱，如無須移除，請填寫「無」】

_____

_____

☐ 已完成檢視/更新受害主機系統與所有應用程式至最新版本(必填)【請說明主要更新之程式名稱，如無須更新，請填寫「皆已更新至最新版本」】

_____

_____

II. 資安管理與教育訓練〈複選〉

☐ 重新檢視機關網路架構適切性

☐ 修正內部資安防護計畫

◎其他相關安全處置【請填寫其他安全處置】

_____

_____

◎已解決時間：_____年_____月____日____時____分

Step5.請填寫機關緊急應變措施-設備異常(請回傳 P1-P3、P13-P14)

◎保留受害期間之相關設備紀錄資料

☐ 其他保留資料或資料處置說明【如未保存資料亦請說明】

_____

_____

◎事件分析與影響評估〈複選〉(最少選填一項，如無對應分析評估結果，請於「影響評估說明補充」欄位說明)

☐ 評估設備影響情況

〈☐無資料遭損毀

☐資料損毀，但可由備份檔案還原

☐資料損毀，且資料無法復原

☐資料損毀，僅可復原部分資料____%〉

☐ 遺失設備存放資料性質說明

〈個人敏感性資料、機密性資料、非機敏性資料，請說明內容〉

_____

_____

_____

☐ 影響評估補充說明

_____

_____

◎封鎖、根除及復原〈複選〉(最少選填一項，如無對應變處理方式，請於「應變措施補充說明」欄位說明)

☐ 毀損資料/系統已恢復正常運作

☐ 完成系統復原測試

☐ 通知事件相關當事人，並依內部資安通報作業向上級呈報【**如遺失設備存有敏感資料，此選項為必填**】

☐ 應變措施補充說明【請填寫補充說明】

_____

_____

Step6.資安事件結案作業-設備異常(請回傳 P1-P3、P13-P14)

六、事件調查與處理：

◎受害資訊設備數量：電腦總計_____臺；伺服器總計_____臺

◎IP 位址(IP Address)(無；可免填)

外部 IP：_____

內部 IP：_____

◎網際網路位址（Web-URL）(無；可免填)：_____

◎作業系統名稱、版本：

□Windows 系列 □Linux 系列 □其他作業平台 版本：_____

◎已裝置之安全機制：

□防火牆 □防毒軟體 □入侵偵測系統 □入侵防禦系統 □其他：_____

◎受害系統是否通過資安管理認證(ISMS)：□是 □否

◎事件發生原因〈單選〉

〈□設定錯誤□設備毀損□系統遭入侵□電力供應異常□人為疏失

□其他_____〉【請說明事件調查情況】

_____

_____

◎補強措施〈複選〉

I. 補強系統/程式安全設定

☐ 檢視資訊設備使用年限

II. 資安管理與教育訓練〈複選〉

☐ 重新檢視機關網路架構適切性

☐ 機關內部全面性安全檢測

☐ 加強內部同仁資安教育訓練

☐ 修正內部資安防護計畫

◎其他相關安全處置【請填寫其他安全處置】

_____

_____

_____

◎已解決時間：_____年_____月____日____時____分

Step5.請填寫機關緊急應變措施-其他(請回傳 P1-P3、P15-P17)

◎保留受害期間之相關設備紀錄資料〈複選〉(最少選填一項，如未保留相關紀錄，請於「其他保留資料或資料處置說明」欄位說明)

☐ 已保存遭入侵主機事件檢視器〈單選〉
〈☐1 個月　1-6 個月　6 個月以上　其他_____〉

☐ 已保存防火牆紀錄〈單選〉
〈☐1 個月　1-6 個月　6 個月以上　其他_____〉

☐ 已保存未授權存在之惡意網頁/留言/檔案/程式樣本，共____個

☐ 其他保留資料或資料處置說明【如未保存資料亦請說明】

_____

_____

◎事件分析與影響評估〈複選〉(最少選填一項，如無對應分析評估結果，請於「影響評估說明補充」欄位說明)經分析已保存之紀錄，是否發現下列異常情形：

☐ 異常連線行為【請列出異常 IP 與異常連線原因，如：存取後台管理頁面】

_____

_____

☐ 異常帳號使用【請列出帳號並說明帳號權限，與判別準則，如：非上班時間帳號異常登入/登出】

_____

_____

☐ 發現資料外洩情況【如：異常打包資料，請說明外洩資料類型/欄位與筆數，如：個人資料/機密性資料/非機敏性資料】

_____

_____

☐ 影響評估補充說明【請填寫補充說明】

_____

_____

◎封鎖、根除及復原〈複選〉(最少選填一項，如無對應變處理方式，請於「應變措施補充說明」欄位說明)

☐ 移除未授權存在之惡意網頁/留言/檔案/程式，共____筆(必填)
【請說明程式名稱或路徑、檔名，如無須移除，請填寫「無」】

_____

_____

☐ 將可疑 IP/Domain Name 列入阻擋清單(必填)【請說明設定阻擋之資訊設備與阻擋之 IP，如無須阻擋，請填寫「無」】

_____

_____

☐ 停用/刪除異常帳號(必填)【請說明停用/刪除之帳號，如無須移除，請填寫「無」】

_____

_____

☐ 暫時中斷受害主機網路連線行為至主機無安全性疑慮

☐ 重新建置作業系統與作業環境，完成日期_____

☐ 惡意程式樣本送交防毒軟體廠商，共__個

☐ 應變措施補充說明【請填寫補充說明】

_____

_____

Step6.資安事件結案作業-其他(請回傳 P1-P3、P15-P17)

六、事件調查與處理：

◎受害資訊設備數量：電腦總計_____臺；伺服器總計_____臺

◎IP 位址(IP Address)(無；可免填)

外部 IP：_____

內部 IP：_____

◎網際網路位址（Web-URL）(無；可免填)：_____

◎作業系統名稱、版本：

☐Windows 系列 ☐Linux 系列 ☐其他作業平台 版本：_____

◎已裝置之安全機制：

☐防火牆 ☐防毒軟體 ☐入侵偵測系統 ☐入侵防禦系統 ☐其他：_____

◎受害系統是否通過資安管理認證(ISMS)：☐是 ☐否

◎事件發生原因〈單選〉

〈☐社交工程☐作業系統漏洞☐弱密碼☐應用程式漏洞

☐網站設計不當☐人為疏失☐設定錯誤☐設備毀損

☐系統遭入侵☐電力供應異常☐其他_____〉【請說明事件調查情況】

_____

_____

◎補強措施〈複選〉

I. 補強系統/程式安全設定〈複選〉

☐ 已完成評估變更透過受害主機登入應用系統密碼之必要性(如：使用受害主機登入之網域帳號密碼、公務系統帳號密碼、郵件帳號密碼等) (必填)

☐ 已完成評估變更受害主機中所有帳號密碼之必要性(含本機管理

者) (必填)

☐ 已完成檢視/更新受害主機系統與所有應用程式至最新版本(必填)
【請說明主要更新之程式名稱，如無須更新，請填寫「皆已更新至最新版本」】

_____

_____

☐ 關閉網路芳鄰功能

II. 資安管理與教育訓練(複選)

☐ 重新檢視機關網路架構適切性

☐ 機關內部全面性安全檢測

☐ 加強內部同仁資安教育訓練

☐ 修正內部資安防護計畫

◎其他相關安全處置【請填寫其他安全處置】

_____

_____

◎已解決時間：_____年_____月____日____時____分

○○○（單位名稱）資通安全事件調查、處理及改善報告範本

通報部門		事件發生時間	
完成通報時間		結案登錄時間	
通報事件等級	■一級　□二級　□三級　□四級		
事件歸類 （請參酌應變紀錄）	□網頁攻擊　■非法入侵　□阻斷服務□設備問題□其他：		
事件等級 判斷依據			
事件說明			
原因肇因			
調查經過			
復原作業			
改善措施			

備　　註			
權　責　人　員		資通安全長	

資通安全演練成果報告

編號：○○○

製表日期：○○○年○○月○○日

<table>
<tr><td colspan="2">演練單位：人事室</td><td rowspan="2">演練時間：○○○年○○月○○日下午○○時○○分至○○○年○○月○○日下午○○時○○分</td></tr>
<tr><td colspan="2">實施單位：稽核小組</td></tr>
<tr><td colspan="2">演練項目</td><td>演練情況概述</td></tr>
<tr><td>1.</td><td>EX：社交工程演練</td><td>寄發社交工程信件，造成人員電腦中毒的通報應變。</td></tr>
<tr><td>2.</td><td>…</td><td>…</td></tr>
<tr><td colspan="3">演練結果</td></tr>
<tr><td colspan="2">合格項目</td><td>EX：依規定進行通報。</td></tr>
<tr><td colspan="2">不合格項目</td><td>EX：未依規定與受影響之其他機關聯繫。</td></tr>
<tr><td colspan="2">待改善項目</td><td>EX：通報紀錄單填寫不完整。</td></tr>
<tr><td colspan="2">其他</td><td>…</td></tr>
<tr><td colspan="3">演練結果檢討與待改善事項</td></tr>
<tr><td colspan="3">(由各單位自行填寫)</td></tr>
</table>