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](http://www.ncert.nat.gov.tw/))通報資安事故，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。

國家資通安全會報傳真專線：(02)27331655 地址：台北市大安區106富陽街116號

國家資通安全會報 諮詢專線：(02)27339922

交通部傳真專線：(02)23820655 副本地址：10052臺北市中正區仁愛路1段50號10F

交通部 諮詢專線：(02)23492832；23492838；23492830

\*注意事項\*

1.「◎」為必填項目；「●及■」代表已勾選。

2.請依通報之資安「事故分類」填寫通報單，並依事故類別回傳通報單內容。

◎填報時間：\_\_\_\_年\_\_\_\_月\_\_\_\_日\_\_\_\_時\_\_\_\_分

|  |
| --- |
| STEP1.**請填寫事故相關基本資料** |
| 一、發生資通安全事故之機關(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  二、機關發生資通安全事故基本資訊：  1.事故發生時間：\_\_\_\_\_年\_\_\_\_月\_\_\_\_日\_\_\_\_時\_\_\_\_分  2.設備資料：  ◎受害主機數量：主機總計\_\_\_\_\_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 □入侵防禦系統 □其他：\_\_\_\_\_\_\_\_\_\_\_\_  ◎資安監控中心(SOC)：  □無□機關自行建置□委外建置 \_\_\_\_\_\_\_\_\_(請提供廠商名稱)  ◎受害系統是否通過資安管理認證(ISMS) □是 □否  ◎資安維護廠商：\_\_\_\_\_\_\_\_\_\_\_(請提供廠商名稱) |
| **STEP2.評估事故影響等級** (「◎」為必填項目；「●及■」代表已勾選) |
| 三、事故影響等級  ◎請分別評估資安事故造成之機密性、完整性以及可用性衝擊：  \*資安事故影響等級為機密性、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) |

|  |
| --- |
| **STEP3.請詳述事故發生過程** (「◎」為必填項目；「●及■」代表已勾選) |
| ◎事故分類與異常狀況：(事故分類為單選項；異常狀況為複選項)  1.🌕網頁攻擊  □網頁置換 □惡意留言 □惡意網頁 □惡意網頁 □釣魚網頁  □網頁木馬 □網站個資外洩  2.🌕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  3.🌕阻斷服務(DoS/DDoS)  □服務中斷 □效能降低  4.🌕設備異常  □設備毀損 □電力異常  5.🌕其他：　　　　　\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  ◎事故說明：  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  ◎是否影響其他政府機關(構)或重要民生設施運作：□是 □否  ◎此事故通報來源：□自行發現 □警訊通知，發布編號：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

事故分類共分5類：  
1.「網頁攻擊」類請填寫p1-p6；  
2.「非法入侵」類請填寫p1-p3及p7-p9；  
3.「阻斷服務」類請填寫p1-p3及p10-p11；  
4.「設備異常」類請填寫p1-p3及p12-p13；  
5.「其他」類請填寫p1-p3及p14-p16

|  |
| --- |
| **Step4.請填寫機關緊急應變措施-網頁攻擊**(請回傳P1-P6) |
| ◎保留資料〈複選〉  □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\_\_\_\_\_〉  □已保存惡意程式樣本，共\_\_\_個  □其他保留資料或資料處罝說明【如未保存資料亦請說明】  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  ◎事故分析與影響評估〈複選〉  □發現異常連線IP【請列出異常IP與異常連線原因，如：存取後台  管理頁面】  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  □發現異常帳號【請列出帳號並說明帳號權限】  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  □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】  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  □發現帳號異常登入/登出紀錄【請提供異常帳號與判別準則】  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  □網站資料庫內容遭竄改  □外洩資料包含機敏性資料，共 \_\_筆，性質為〈單選〉  　□個人敏感性資料  □機密性資料  □其他【請說明外洩資料類型】  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  □外洩資料包含非機敏性資料，共\_\_\_筆，請說明內容【請簡述資料  欄位】  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  □影響評估說明補充【請填寫補充說明】  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  ◎封鎖、根除及復原〈複選〉  □移除惡意網頁/留言，共\_\_筆  □移除惡意程式【請說明程式名稱或路徑、檔名】  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  □將異常連線IP列入阻擋清單【請說明設定阻擋之資訊設備與阻擋  之IP】  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  □停用/刪除異常帳號【請說明停用/刪除之帳號】  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  □移除未授權存在之程式/檔案，共\_\_\_個  □移除網站外洩資料  □通知事故相關當事人，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，完成日期日期選單  □重新建置作業系統與作業環境，完成日期日期選單  □應變措施補充說明【請填寫補充說明】  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **Step5.評估是否需要外部支援-網頁攻擊**(請回傳P1-P6) |
| 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）  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **STEP6.資安事故結案作業-網頁攻擊**(請回傳P1-P6) |
| ◎事故發生原因〈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□其他\_\_\_\_\_\_〉  ◎補強措施〈複選〉   * + - 1. 補強系統/程式安全設定   □變更透過受害主機登入應用系統之密碼(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)  □變更受害主機中所有帳號之密碼(含本機管理者)  □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)【請說明主要更新之程式名稱】  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  □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)   * + - 1. 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】  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  五、已解決時間：\_\_\_\_\_年\_\_\_\_\_月\_\_\_\_日\_\_\_\_時\_\_\_\_分 |
| **簽核作業：(1/2級資訊主管決行；3/4級資訊安全長核章)**  **通報機關(單位)**  **資安聯絡人：　　 　 　 資安主管：　　　　　 資訊安全長或授權人：** |
| **審核機關(單位): (3/4級陳報資訊安全長)**  **資安聯絡人：　　　 資安主管：　　　　　 資訊安全長或授權人：** |
|  |
| **Step4.請填寫機關緊急應變措施-非法入侵**(請回傳P1-P3、P7-P9) |
| ◎保留資料〈複選〉  □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\_\_\_\_\_〉  □已保存惡意程式樣本，共\_\_個  □其他保留資料或資料處罝說明【如未保存資料亦請說明】  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  ◎事故分析與影響評估〈複選〉  □發現設備連線至可疑IP/Domain Name【請說明連線資訊設備用途與  目的IP/Domain Name】  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  □發現受害主機帳號異常登入/登出紀錄【請提供異常帳號與判別準  則】  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  □發現異常帳號【請列出帳號並說明帳號權限】  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  □發現資料外洩情況(如：異常打包資料)【請說明外洩資料內容】  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  □影響評估補充說明【請填寫補充說明】  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  ◎封鎖、根除及復原〈複選〉  □移除惡意程式【請說明程式名稱或路徑、檔名】  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  □將可疑IP/Domain Name列入阻擋清單【請說明設定阻擋之資訊設備  與阻擋之IP/Domain】  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  □停用/刪除異常帳號【請說明停用/刪除之帳號】  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  □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  □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】  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

|  |
| --- |
| **Step5.評估是否需要外部支援-非法入侵**(請回傳P1-P3、P7-P9) |
| 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）  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

|  |
| --- |
| **Step6.資安事故結案作業-非法入侵**(請回傳P1-P3、P7-P9) |
| ◎事故發生原因〈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□其他\_\_\_\_\_\_\_〉【請說明事故調查情況】  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  ◎補強措施〈複選〉   1. 補強系統/程式安全設定〈複選〉   □已更新受害主機系統與所有應用程式至最新版本【請說明主要更新  之程式名稱】  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  □變更透過受害主機登入應用系統之密碼(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)  □變更受害主機中所有帳號之密碼(含本機管理者)  □關閉郵件伺服器Open Relay功能  □關閉網路芳鄰功能   1. 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】  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  五、已解決時間：\_\_\_\_\_年\_\_\_\_\_月\_\_\_\_日\_\_\_\_時\_\_\_\_分 |
| **簽核作業：(1/2級資訊主管決行；3/4級資訊安全長核章)**  **通報機關(單位)**  **資安聯絡人：　　 　 　 資安主管：　　　　　 資訊安全長或授權人：** |
| **審核機關(單位): (3/4級陳報資訊安全長)**  **資安聯絡人：　　　 資安主管：　　　　　 資訊安全長或授權人：** |

|  |
| --- |
| **Step4.請填寫機關緊急應變措施-阻斷服務(DoS/DDoS)**(請回傳P1-P3、P10-P11) |
| ◎保留資料〈複選〉  □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\_\_\_\_\_〉  □已保存惡意程式樣本，共\_\_個  □其他保留資料或資料處罝說明【如未保存資料亦請說明】  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  ◎事故分析與影響評估〈複選〉  □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〉  □阻擋攻擊來源IP【請說明設定阻擋之資訊設備與阻擋之IP範圍  /Domain】  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  □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】  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

|  |
| --- |
| **Step5.評估是否需要外部支援-阻斷服務(DoS/DDoS)**(請回傳P1-P3、P10-P11) |
| 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）  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **Step6.資安事故結案作業-阻斷服務(DoS/DDoS)**(請回傳P1-P3、P10-P11) |
| ◎補強措施〈複選〉   1. 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  □移除主機/伺服器不必要服務功能【請說明服務功能名稱】  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  □更新受害主機系統與所有應用程式至最新版本【請說明主要更新之  程式名稱】  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   1. 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】  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  五、已解決時間：\_\_\_\_\_年\_\_\_\_\_月\_\_\_\_日\_\_\_\_時\_\_\_\_分 |
| **簽核作業：(1/2級資訊主管決行；3/4級資訊安全長核章)**  **通報機關(單位)**  **資安聯絡人：　　 　 　 資安主管：　　　　 　資訊安全長或授權人：** |
| **審核機關(單位): (3/4級陳報資訊安全長)**  **資安聯絡人：　　　 資安主管：　　　　　 資訊安全長或授權人：** |

|  |
| --- |
| **Step4.請填寫機關緊急應變措施-設備異常**(P1-P3、P12-P13) |
| ◎保留資料〈複選〉  □其他保留資料或資料處罝說明【如未保存資料亦請說明】  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  ◎事故分析與影響評估〈複選〉  □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\_\_\_\_%〉  □影響評估補充說明  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  ◎封鎖、根除及復原〈複選〉  □毀損資料/系統已恢復正常運作  □完成系統復原測試  □應變措施補充說明【請填寫補充說明】  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

|  |
| --- |
| **Step5.評估是否需要外部支援-設備異常**(P1-P3、P12-P13) |
| 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）  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

|  |
| --- |
| **Step6.資安事故結案作業-設備異常**(P1-P3、P12-P13) |
| ◎事故發生原因〈單選〉  〈□設定錯誤□設備毀損□系統遭入侵□電力供應異常  □其他\_\_\_\_\_\_\_〉【請說明事故調查情況】  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  ◎補強措施〈複選〉   1. 補強系統/程式安全設定   □檢視資訊設備使用年限   1. 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】  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  五、已解決時間：\_\_\_\_\_年\_\_\_\_\_月\_\_\_\_日\_\_\_\_時\_\_\_\_分 |
| **簽核作業：(1/2級資訊主管決行；3/4級資訊安全長核章)**  **通報機關(單位)**  **資安聯絡人：　　 　 　 資安主管：　　　　 　資訊安全長或授權人：** |
| **審核機關(單位): (3/4級陳報資訊安全長)**  **資安聯絡人：　　　 資安主管：　　　　 　資訊安全長或授權人：** |

|  |
| --- |
|  |
| **Step4.請填寫機關緊急應變措施-其他**(P1-P3 、P14-P16) |
| ◎保留資料〈複選〉  □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\_\_\_\_\_〉  □已保存惡意程式樣本，共\_\_個  □其他保留資料或資料處罝說明【如未保存資料亦請說明】  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  ◎事故分析與影響評估〈複選〉  □發現設備連線至可疑IP/Domain Name【請說明連線資訊設備用途與  目的IP/Domain Name】  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  □發現受害主機帳號異常登入/登出紀錄【請提供異常帳號與判別準  則】  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  □發現異常帳號【請列出帳號並說明帳號權限】  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  □發現資料外洩情況(如：異常打包資料)【請說明外洩資料內容】  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  □影響評估補充說明【請填寫補充說明】  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  ◎封鎖、根除及復原〈複選〉  □移除惡意程式【請說明程式名稱或路徑、檔名】  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  □將可疑IP/Domain Name列入阻擋清單【請說明設定阻擋之資訊設備  與阻擋之IP/Domain】  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  □停用/刪除異常帳號【請說明停用/刪除之帳號】  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  □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】  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

|  |
| --- |
| **Step5.評估是否需要外部支援-其他**(P1-P3 、P14-P16) |
| 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）  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **Step6.資安事故結案作業-其他**(P1-P3 、P14-P16) | |
| ◎事故發生原因〈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\_\_\_\_\_\_\_〉【請說明事故調查情況】  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  ◎補強措施〈複選〉   1. 補強系統/程式安全設定〈複選〉   □已更新受害主機系統與所有應用程式至最新版本【請說明主要更新  之程式名稱】  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  □變更透過受害主機登入應用系統之密碼(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)  □變更受害主機中所有帳號之密碼(含本機管理者)  □關閉網路芳鄰功能   1. 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】  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  五、已解決時間：\_\_\_\_\_年\_\_\_\_\_月\_\_\_\_日\_\_\_\_時\_\_\_\_分 | |
| **簽核作業：(1/2級資訊主管決行；3/4級資訊安全長核章)**  **通報機關(單位)**  **資安聯絡人：　　 　 　 資安主管：　　　　　 資訊安全長或授權人：** | |
| **審核機關(單位): (3/4級陳報資訊安全長)**  **資安聯絡人：　　　 資安主管：　　 　　　資訊安全長或授權人：** | |