聯防監控

事件紀錄回傳標準作業程序

(V1.3)

國家資通安全會報技術服務中心

中華民國106年7月

目　次

圖 目 次

修訂歷史紀錄

版次	生效日期	修 訂 說 明
V1.0	103/01/10	新制訂
V1.1	103/02/06	二線情蒐服務更名為二線監控
V1.2	106/04/11	二線監控更名為聯防監控
V1.3	106/07/25	行政院資通安全辦公室更名為行政院資通安全處；連通帳號申請書修訂

1. 前言

本文件主要說明各級政府機關(構)配合技術服務中心(以下簡稱技服中心)，依國家資通安全通報應變作業綱要第四章第一節第一項第九款，建立定期性監控情蒐回傳機制，辦理外部 SOC 事件紀錄情資回傳技服中心聯防監控平台之作業程序，涵蓋連通測試作業與傳送稽核作業。聯防監控負有彙整及關聯分析國家級資安防護作業之任務，並研究分析全國網路威脅趨勢，各級政府機關不論委外 SOC 或自建 SOC 在系統觸發並記錄事件資料時，應即回傳資料至技服聯防監控平台，針對各項系統操作說明如下：

- 事件紀錄資料上傳聯防監控平台連通測試作業
- 事件紀錄資料稽核檢測作業

2. 事件紀錄資料上傳聯防監控平台連通測試作業標準流程

委外或自建 SOC(以下簡稱上傳單位)之事件資料管理人員進行資安監控事件紀錄資料上傳時，應參照上傳事件資料連通測試與稽核標準流程圖進行資料上傳，確認資安事件資料成功匯入聯防監控平台之資料倉儲中，此外週期性進行資料稽核檢測確保資料一致性，上傳事件資料連通測試與稽核標準流程詳見圖 1。各流程說明如下：

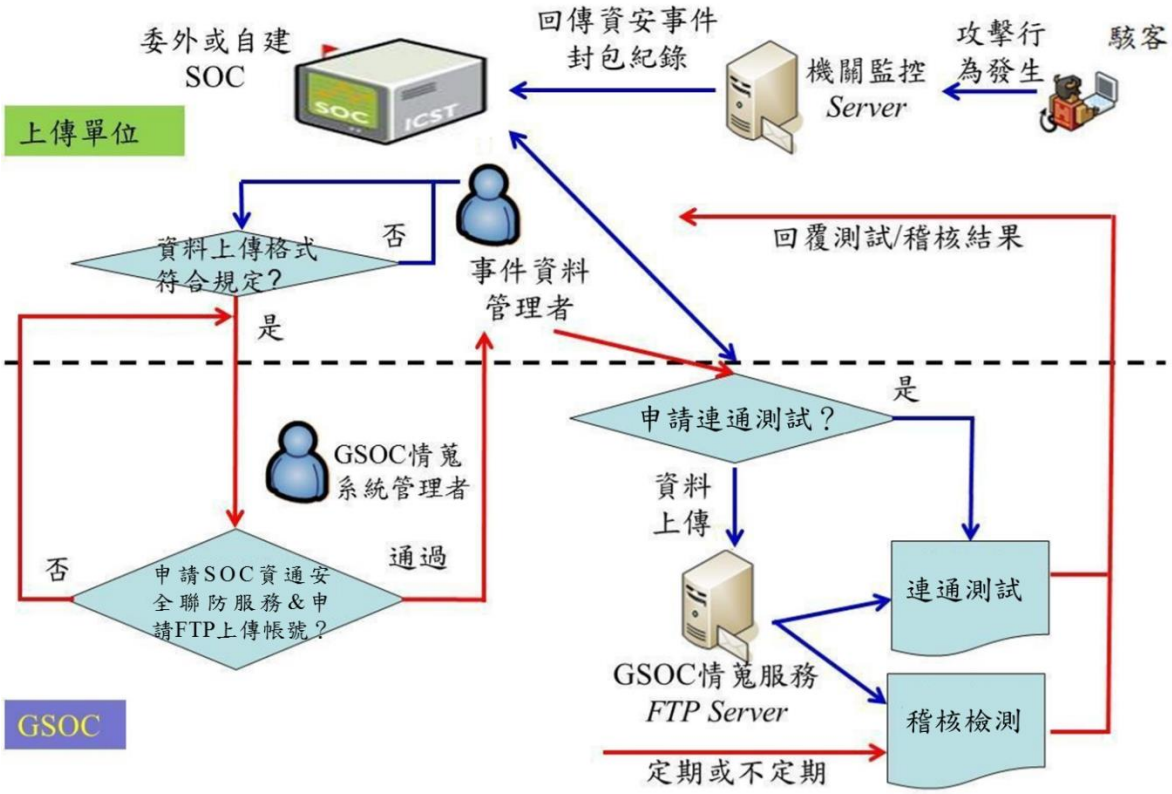

圖1　上傳事件資料連通測試與稽核標準流程

資料來源：本計畫整理

(1)檢核事件資料上傳格式

上傳單位之事件資料管理人員對於上傳資料格式內容先進行相容性檢測，標準格式應依循附件 1 事件資料數據回傳欄位與格式規範，自行對其事件資料進行格式相容轉換，事件資料管理人員須檢核其回傳資料是否符

合規範並確認正確無誤。

(2)申請事件資料 **FTP** 上傳帳號

聯防監控平台之事件資料收集方法是由各上傳單位以 FTPS 方式即時上傳事件資料，聯防監控平台再自動匯入整體資料倉儲中。上傳機關在進行連通測試之前須填具 SOC 資通安全聯防服務申請表(參考附件 4)，以公文書（含申請書）寄送或傳真向技服中心資訊研析組提出申請，資訊研析組於檢驗核定通過後，填入 FTPS 網址與帳號資訊回覆申請單位，密碼另以不同通訊管道另行通知申請人。

(3)上傳資料並申請連通測試

上傳單位於收到.聯防監控資訊回傳作業帳號申請書與 FTPS 上傳帳號申請通過回覆後，為利於聯防監控平台關聯分析研究需要，各上傳單位應即上傳機關服務列表與關聯規則 ID 對照總表至給定 FTPS 上傳目錄位置，機關服務列表得依循附件 2 機關服務列表範例，關聯規則 ID 對照總表得依循附件 3 關聯規則 ID 對照總表範例。始得開始即時上傳事件測試資料，並自行檢驗確定是否上傳成功，上傳檔案命名方式應參考下列規範：

檔名命名方式：XXXXXXX.xml(其中 XXXXXXX 與 Event_ID 一致，Event_ID 請參照附件 1 欄位編號 2 之 Event_ID 說明)。

上傳單位確定資料上傳無誤，且上傳至少一天測試資料或一筆事件測試資料後，填具連通測試申請表(參照附件 5)，得以公文書（含申請書）寄送或傳真向技服中心資訊研析組提出連通測試申請，資訊研析組應依連通測試書逐項測試是否符合規定，測試完畢後填入測試紀錄及結果回覆上傳單位。

3. 上傳資料稽核檢測

技服中心資訊研析組得定期或不定期進行上傳單位之資料一致性檢驗。主要作業分為不定期與定期查核作業：

不定期查核作業：當聯防監控平台之系統管理員於匯入上傳單位之事件資料作業過程中，出現機關或事件關聯比對錯誤時。

定期查核作業：聯防監控平台得每半年依資料上傳定期稽核檢測步驟

Checklist(參考附件 6)逐項測試是否符合要求

上述二項作業若發現問題須改正，技服中心資訊研析組應開立上傳稽核問題紀錄單(參照附件 7) ，得以郵件或書面通知上傳單位限期改善，逾期未改善者，技服中心得暫停或終止上傳單位之 FTPS 帳號與上傳服務作業，並對外公告上傳單位之服務被暫停或終止之資訊。

4. 附件

附件1事件資料數據上傳欄位與格式規範

國家資通安全會報 技術服務中心

聯防監控資訊回傳數據欄位與格式規範

編號	Field Name	參考中文描述(勿以此為回傳名稱)	格式	欄位必須性(M 必填 O 選擇)	說明
1	Organization	發送單位	String(max 40)	M	發送事件單之單位或組織代號，如中華電信、ACER 等
2	Event_ID	事件單(Incident)ID	String(max 40)	M	事件單(Incident)編號，此為發送事件單之單位的事件單編號，該欄位亦為檔案名稱(如補充說明 4)。
3	Customer_Name	機關名稱	String(max 255)	M	監控機關完整名稱(中央政府機關名稱請參照 http://www.gov.tw/OrgInfo/ORPF-GOV-01.aspx)
4	Customer_ID	機關代碼	中央政府機關之 OID	M	監控機關之 OID 編號
5	Subject	事件單主旨	String(max255)	M	事件單簡述主旨(Subject)
6	Base_Event_ID	事件(Event)ID	String(max40)	O	發送事件單之單位關聯事件單之編號

編號	Field Name	參考中文描述(勿以此為回傳名稱)	格式	欄位必須性(M 必填 O 選擇)	說明
7	Event_Name	事件名稱	String(max 255)	M	事件單名稱(暫依各單位之定義)
8	Start_Time	事件發生時間	String(max 25) YYYY-MM-DD HH:MM:SS.X	M	事件觸發之時間(原始第一筆時間)
9	End_Time	事件結束時間	String(max 25) YYYY-MM-DD HH:MM:SS.X	M	事件結束時間(發送機關時間)
10	Connector_Translated_Zone_Reference_ID	事件來源	String(max40)	O	被監控機關觸發事件單之原始事件搜集器 ID 與名稱
11	Source_Address	來源 IP	String(max40)	M	事件單來源位址
12	Target_Address	目標 IP	String(max40)	M	事件單目標位址
13	Source_Port	來源 PORT	String(max40)	O	事件單來源使用埠
14	Target_Port	目標 PORT	String(max40)	O	事件單目標使用埠
15	Source_ Geo_Descriptor	來源 IP 經緯度	String(max40) 格式(xxx,xxx)	O	事件單來源經緯度
16	Target_ Geo_Descriptor	目標 IP 經緯度	String(max40) 格式(xxx,xxx)	O	事件單目標經緯度
17	Event_ Attacking_ Technical	手法研判	String(max 255)	O	事件單中註明之攻擊手法

編號	Field Name	參考中文描述(勿以此為回傳名稱)	格式	欄位必須性(M 必填 O 選擇)	說明
18	Events_ Description	事件描述	String(max 255)	M	事件單中註明之事件過程
19	Event_Message	處理說明	String(max 255)	M	事件單中發送單位之處理建議
20	Event_ Vulnerability	弱點資訊	String(max 255)	O	本事件單之弱點補充資訊如：弱點類別、弱點名稱、CVE-ID 等
21	Event_Severity	影響等級	String(max 20)	M	本事件單之風險嚴重度，預設分 10 等級
22	Device_ Translated_Zone Reference_ID	觸發設備	String(max 255)	O	本事件單之來源 Log 設備名稱(型號為補充內容)
23	Triggered_Rule Name	觸發規則	String(max 255)	O	本事件單之來源 Log 設備規則名稱
24	Correlated_Rule Name	關聯規則名稱	String(max 255)	O	觸發關聯規則名稱
25	Correlated_Rule ID	關聯規則 ID	String(max 255)	O	觸發關聯規則編號(關聯規則編碼)
26	Correlated_Raw Event_ID	關聯事件 ID	String(max 255)	O	觸發關聯規則之紀錄編號
27	Aggregated_ Count	關聯事件數	String(max 40)	M	觸發關聯規則之彙總記錄數量
28	Attachment	附件(如補充說明 6)	UTF-8 編碼	O	觸發關聯規則之附檔說明

補充說明：

1.資訊回傳欄位應至少包含上述欄位內容，實際輸出時依狀況不同會額外增加其他欄位內容，但以不影響 CSV/XML 資訊結構為主。

2.XML 編碼語言請設定為 UTF-8。

3.回傳數據欄位 Field Name 要求與聯防 SOC Field Name 一致(勿以中文欄位 回傳)，Field Name 中間請加底線，勿留空格。

4.回傳檔名命名方式: Event_ID.xml(如格式欄位編號 2)。

5.必填欄位若無回傳值，內容請回傳 NULL 值。

6.上傳檔案放置於 incident 目錄，附件放置於 attachment 目錄。

附件2機關服務列表範例 (檔名範例: (上傳單位名稱)_Service_Lists.csv)

序號	機關之 OID 代碼	機關名稱
1	2.16.886.101.20002	總統府
2	2.16.886.101.20003	行政院
3	2.16.886.101.20006	考試院
4	2.16.886.101.20007	監察院
5	2.16.886.101.20003.20025	中央銀行
6	2.16.886.101.20003.20033	行政院大陸委員會
7		

(若表格資料列不足請自行增加**)**

附件3 關聯規則 ID 對照總表範例(檔名範例: (上傳單位名稱)_Rules_ID.csv)

關聯規則 ID	關聯規則名稱	備註說明
144	FTP ADMw0rm ftp login attempt	
224	DDOS Stacheldraht server spoof	
230	DDOS shaft client login to handler	
262	DNS EXPLOIT x86 Linux overflow attempt	
286	POP3 EXPLOIT x86 BSD overflow	
309	EXPLOIT sniffit overflow	

(若表格資料列不足請自行增加**)**

附件4SOC 資通安全聯防服務申請表

行政院國家資通安全會報技術服務中心

聯防監控資訊回傳作業帳號 申請／異動書

以下粗框欄位請以☑勾選

<table>
<tr><td colspan="4">用戶類型: □自建 SOC 單位 □SOC 業者 □其他：</td></tr>
<tr><td colspan="3">□新申請 □增加服務項目 □終止服務 □暫停服務
□恢復服務 □其他：________________</td><td>申請日期：____年____月____日</td></tr>
<tr><th colspan="4">申請機關／單位／業者資料</th></tr>
<tr><td>申請單位</td><td colspan="2"></td><td>機關 OID 編號：（無 OID 者不需填寫）</td></tr>
<tr><td colspan="4">地址：□□□ （縣市） （鄉鎮市區） （路街） 段 巷 弄 號 樓之</td></tr>
<tr><td>申請人</td><td colspan="3">姓名： 部門/職稱： 電話：( ) 分機
傳真：( ) E-mail：</td></tr>
<tr><td>主要聯絡人</td><td colspan="3">姓名： 部門/職稱： 電話：( ) 分機
傳真：( ) E-mail：</td></tr>
<tr><td>次要聯絡人</td><td colspan="3">姓名： 部門/職稱： 電話：( ) 分機
傳真：( ) E-mail:</td></tr>
<tr><th colspan="4">請確認下列事項：</th></tr>
<tr><td>□是</td><td>□否</td><td colspan="2">（一）是否 貴單位相關人員皆已瞭解資通安全聯防服務內容</td></tr>
<tr><td>□是</td><td>□否</td><td colspan="2">（二）是否備妥相關資料（公函、網路架構圖）</td></tr>
<tr><td>□是</td><td>□否</td><td colspan="2">（三）是否明確指派聯絡窗口</td></tr>
<tr><td>□是</td><td>□否</td><td colspan="2">（四）是否檢附受監控機關列表</td></tr>
<tr><td colspan="2"></td><td colspan="2">（五）其他需求說明：________________
________________</td></tr>
<tr><th colspan="2">申請機關/單位印信</th><th colspan="2"></th></tr>
<tr><td colspan="2"></td><td colspan="2"></td></tr>
<tr><th colspan="2">以下由國家資通安全會報技術服務中心填寫</th><th colspan="2">注意事項</th></tr>
<tr><td colspan="2">用戶編號：
□啟用 □暫停 □恢復 □終止
□其他：____________

日期： 年 月 日</td><td colspan="2">申請機關/單位必須使用公文書（含本申請書）寄送或傳真至下列聯絡方式進行書面申請。</td></tr>
</table>

服務專線：02-2733-9922（24 小時） 傳真：02-2733-1655 資訊研析組收

聯絡地址：106 台北市大安區富陽街 116 號 資訊研析組收

● 自建 SOC 單位與 SOC 業者	
FTP 帳號申請資訊	
申請類型	□新增帳號 □帳號異動 □刪除帳號
使用期間	□長期使用 □短期使用 ____年____月____日至____年____月____日
以下由國家資通安全會報技術服務中心填寫	
數據上傳位址/目錄	
FTP 使用者帳號	

立同意書人(以下簡稱「本人」)，茲同意國家資通安全會報技服中心基於聯防監控之目的範圍內，於計畫終止前 1 個月內，得以電子與紙本方式進行蒐集、處理及利用本人之個人資料(辨識個人者資料包含姓名、E-MAIL、電話、傳真、地址等)，其使用對象為行政院及其委辦單位，使用地區為中華民國境內。本人瞭解依法得就上開之個人資料行使個人權利，並瞭解不同意提供或要求停止蒐集、處理或利用以及刪除上開資料，將導致前述目的無法達成，有可能影響個人或公務資訊正確登錄與訊息傳遞。本人可依「個人資料保護法」第 3 條規定行使個資當事人權利，包含查詢或請求閱覽、製給複製本、補充或更正、停止蒐集、處理或利用及刪除等作業。

□本人_____(請簽名)已詳閱並充分明瞭同意上述事項□本人不同意上述事項

附件5聯防監控連通測試書

國家資通安全會報技術服務中心

聯防監控連通測試書

測試單位(回傳單位)：_____

測試機關 OID：_____

測試起始時間：_____

測試完成時間：_____

聯防監控測試環境版本/IP： 1.0/_____

連通測試單位測試數據位址/目錄：117.56.7.8 /_____

第一階段：測試單位提供數據說明文件予 ICST

由測試單位提供測試資料相關說明與對應文件(檔)至 ICST，本測試階段在查驗測試數據之文件說明是否提供足夠與正確資訊供第二階段測試使用。查驗文件及內容包括：

測試項目	Check (OK/Fail)	備註
1-1 測試單位是否定期回傳更新機關服務列表(機關服務列表.doc)？ (含附件,OID,名稱)		
1-2 測試單位是否回傳更新關聯事件與 ID 對照表(關聯事件 ID 對照表.doc)，機關 ID 對照資料是否齊備無重複？ (含附件)		

第二階段：連通測試步驟

由連通測試單位透過 ftps 回傳資料至相對應位置，再由 ICST 之聯防監控系統自動匯入資料庫中，本階段在測試連通測試單位的數據傳送是否正常，並驗證 ICST 是否可順利整合匯入巨量資料倉儲中。

測試項目	Check (OK/Fail)	備註
2-1 連通測試單位傳送數據，數據是否正確回傳？		
2-2 連通測試單位傳送數據，傳送週期是否在發生時間 1 小時內？		
2-3 連通測試單位傳送資料格式是否通過 XSD 驗證？		
2-4 測試單位是否定符合機關名稱 OID 格式？		

測試結果: □通過 □未通過 日期: _____

測試員: _____

聯防監控業務承辦人: _____

附件6 資料上傳定期稽核檢測步驟 Checklist

稽核檢測編號：_____

上傳單位：_____

測試機關 OID：_____

測試起始時間：_____

測試完成時間：_____

測試完成時間：_____

測試項目	Check (OK/Fail)	備註
2-1 與測試機關徵詢勾稽，事件資料總數是否與上傳資料一致？內容一致?		
2-2 是否即時更新機關服務列表、關聯規則 ID 對照總表？		

測試結果: □通過 □未通過　　日期: _____

測試員: _____

附件7稽核問題紀錄單

問題單編號		問題單開立時間	
問題名稱			
問題描述	上傳單位名稱		
	檢測形態		
	發生時間		
	問題嚴重性	□高 □中 □低 □建議	
	測試員		
	事件描述		
建議措施			
參考資料	附件 1：稽核檢測紀錄單資訊(XXXXX)。		
矯正紀錄	覆驗日期: _____ □通過 □未通過 測試員:_____		
	覆驗日期: _____ □通過 □未通過 測試員:_____		
	覆驗日期: _____ □通過 □未通過 測試員:_____		
是否結案	□是 □否 結案日期: _____		

附件 1：稽核檢測紀錄單資訊(XXXXX)

複製資料上傳稽核檢測步驟 Checklist 之檢測紀錄