政府領域聯防監控作業規範

國家資通安全研究院

中華民國112年6月

修訂歷史紀錄表

項次	版次	日期	說明
1	V1.0	108/04/29	新編
2	V2.0	108/06/28	連通測試申請新增電子郵件或傳真
3	V3.0	109/07/20	定義資安監控單與情資分析單
4	V4.0	109/11/12	資安監控情資回饋能量列舉說明
5	V5.0	110/5/1	調整監控有效性驗證指標
6	V6.0	110/12/27	修訂新版格式連通測試和申請說明
7	V7.0	112/1/1	國家資通安全研究院組織更新
8	V8.0	112/5/4	有效性指標用詞調修
9	V9.0	112/6/13	更新國家資通安全研究院聯絡地址

國家資通安全研究院整理

目　次

表目次

圖 目 次

1. 前言

依資通安全情資分享辦法與資通安全責任等級分級辦法，公務機關應完成資通安全威脅偵測管理機制與惡意偵查或情蒐活動相關情資，並持續維運及依主管機關指定之方式提交監控管理資料。

1.1.目的

本規範說明公務機關配合國家資通安全研究院(以下簡稱本院)，不論自行監控或委外監控，在系統觸發並記錄事件資料時，應即回傳資安監控情資至本院聯防監控平台，有效推動資訊安全之運行，預防資安事件發生。

1.2.適用對象

本規範適用對象為執行資安聯防監控作業的公務機關與資安託管服務供應商。

本規範所指之公務機關係指依法行使公權力之中央、地方機關（構）或公法人，但不包括軍事機關及情報機關。

2. 政府領域聯防監控說明

2.1.政府領域角色權責與分工

政府聯防監控依據公務機關回傳的資安監控情資，經過趨勢統計、分類分群及分析預測，建立政府資安情境認知，提供整體情報給 N-SOC，支援政府資安決策與推動公私資安協同合作，詳見圖 1。

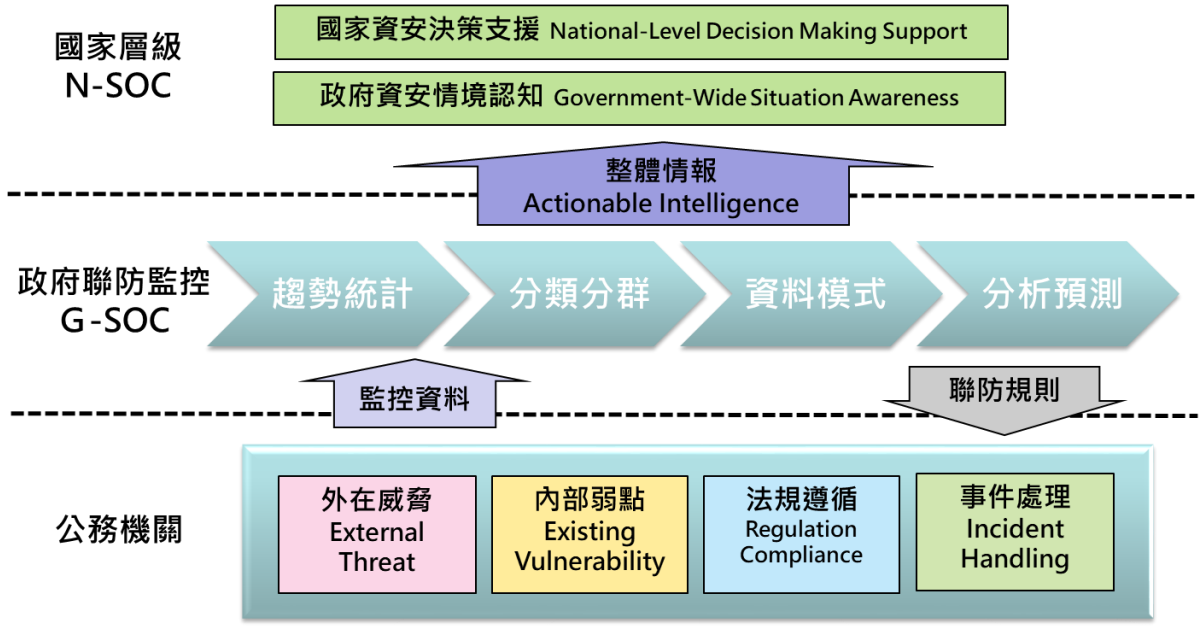

圖1　各層級角色權責與分工

資料來源：本院整理

公務機關應依據權責分工建置資安監控防護機制，並針對資通安全威脅偵測管理機制產製之資訊提供給政府聯防監控平台；政府聯防監控依據收容的資安監控情資進行整體政府領域之資安威脅情資分析、聯防回饋情資產製並分享，相關工作詳見表 1。

表1　各層級聯防必要工作項目

公務機關	政府聯防監控 G-SOC

● 建置資安監控防護機制、日誌收容及分析 ● 回傳資安監控單 ● 回傳情資分析單 ● 回傳監控設備狀況單	● 產製區域資安指標情資 ● 產製區域聯防監控分析結果 ● 分享區域資安指標情資 ● 分享區域聯防監控分析情資

資料來源：本院整理

2.2.政府領域聯防監控情資收容架構

機關依權責與分工完成聯防必要工作項目，由監控執行單位進行監控情資回傳作業，收容架構詳見圖 2，監控資料應以 STIX 2.1 格式封裝，狀況單以 CSV 格式回傳，傳輸收容方式為 FTPS。

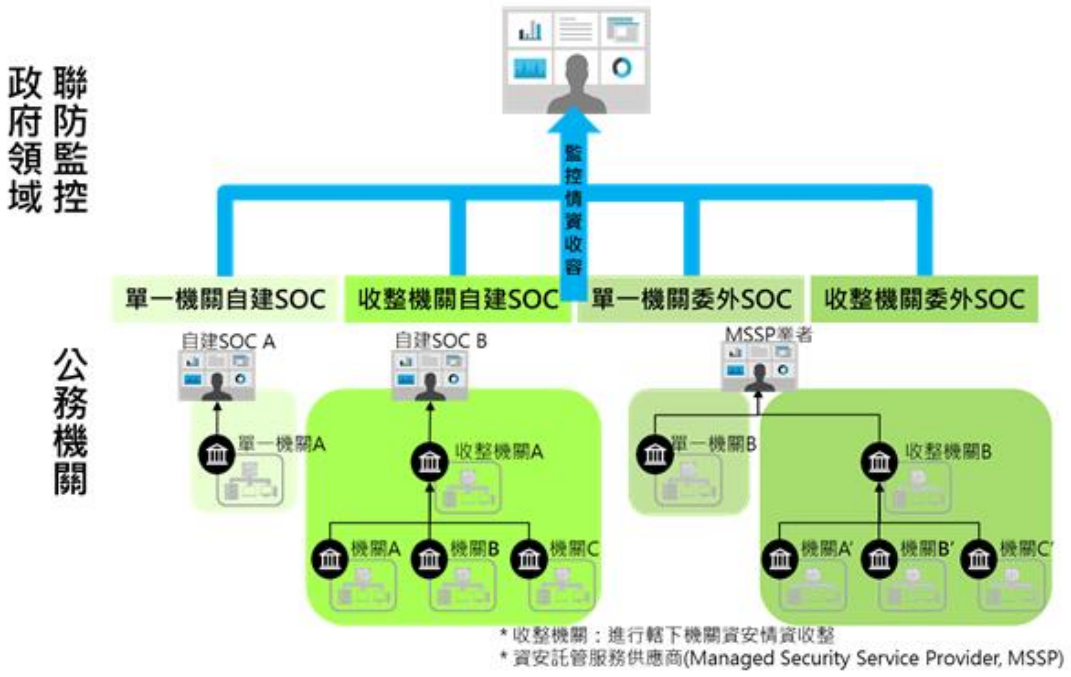

圖2　政府領域聯防監控情資收容架構

資料來源：本院整理

2.3.聯防監控情資內容

聯防監控情資包含資安監控單、情資分析單及監控設備狀況單 3 類資訊，情資內容說明詳見表 2，涵蓋資通安全防護、端點偵測及應變機制、目錄服務系統及核心資通系統之資通設備紀錄及資訊服務或應用程式紀錄。監控執行單位應即時回傳資安監控單和情資分析單，格式規範詳見「聯防監控資安情資回傳 STIX 格式規範」文件，於每個月 5 號前回傳上個月的監控設備狀況單，監控設備狀況單格式規範詳見附件 1。

表2　聯防監控情資內容

項次	情資內容	情資說明
1	資安監控單	資安監控機制整合產製之資安監控單(例如：incident)
2	情資分析單	SOC 分析人員對「資安監控單」進行影響性評估，提供給客戶進行分析之情資(例如：ticket)
3	監控設備狀況單	所有監控設備之監控狀況資訊

資料來源：本院整理

聯防監控情資單於 FTPS 存放目錄位置：資安監控單放置於 incident 目錄；情資分析單放置於 ticket 目錄；監控設備狀況單放置於 status 目錄；端點偵測及應變機制放置於 EDR 目錄。

3. 聯防監控情資單回傳作業規範

機關需於資通安全作業管考系統提報資安監控作業辦理事項，包含：監控機關列表與資安防護項目，並回傳資安情資，詳見圖 3。

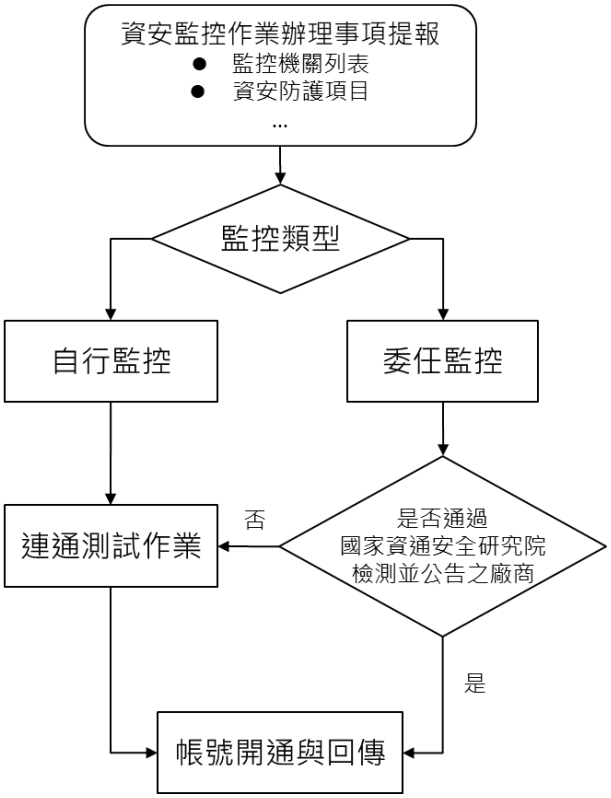

圖3　聯防監控提報與情資回傳作業

資料來源：本院整理

●自行監控機關

– 完成連通測試後，辦理帳號開通與情資回傳

●委任監控機關

– 責成 SOC 監控廠商辦理情資回傳

■ 通過本院連通測試並公告之 SOC 監控廠商，辦理帳號開通與情資回傳

■ 尚未通過本院連通測試並公告之 SOC 監控廠商

- ◆ 機關需責成 SOC 監控廠商辦理連通測試，待通過連通測試後，方可辦理帳號開通與情資回傳。

聯防監控情資回傳作業程序包含連通測試作業與監控有效性驗證作業，相關說明如下：

3.1.連通測試作業

自行監控機關或 SOC 監控廠商(以下簡稱上傳單位)之事件資料管理人員進行資安監控情資回傳前，應依規定進行連通測試，確認相關資料成功回傳至聯防監控收容平台。

3.1.1. 申請連通測試

聯防監控平台之監控資料收集方法係由上傳單位以 FTPS 方式，即時回傳資安監控情資至聯防監控平台。上傳單位於進行連通測試前，應填具資安情資回傳連通測試申請單(參考附件 2)，郵寄、電子郵件或傳真給本院提出申請，內容包含申請單位、聯絡人及 IP 等相關資料；本院於帳號和防火牆開通後，將測試系統位址、帳號及密碼以不同通訊管道另行通知上傳單位。

3.1.2. 連通測試

聯防監控資安情資格式與內容應依循「聯防監控資安監控情資回傳 STIX 格式規範」規範，針對資安監控情資進行格式相容轉換與對應，並將資安監控單、情資分析單及監控設備狀況單分別上傳至對應的資料夾。

本院於帳號開通一個月內，檢核其回傳資料是否符合規範，將測試結果和報告回覆上傳單位，連通測試項目參考附件 3。

連通測試未通過之申請測試單位，最快於測試結束一個月後方得再次申請連通測試；連通測試通過之委任廠商，將會於本院網站公告。

3.2.正式回傳作業辦理

通過連通測試後，本院與上傳單位確認正式回傳來源主機位址，並於管理規則開通後，將正式連通方式另行通知上傳單位，上傳單位應於一周內開始回傳聯防監控情資。

3.3.監控有效性驗證作業

為確保監控之有效性，本院針對回傳能力、偵測能力及情資品質進行驗證，每月 6 日提供前一月份之監控有效性驗證結果予上傳單位，有疑慮之上傳單位得於當月 20 日前提出申覆，並每季(1 月、4 月、7 月及 10 月)於聯防監控月報呈現，驗證指標詳見表 3。

表3　監控有效性驗證指標

項目	分析指標	說明
1.回傳能力	1.1 資安監控情資格式正確率	1.1.1 依據「聯防監控資安監控情資回傳 STIX 格式規範」規定之「資安監控單」與「情資分析單」格式進行正確性驗證
	1.2 資安防護項目回傳率	1.2.1 依據 SOC 業者回傳「監控設備狀況單」之資安防護項目資訊，評估其監控偵測之回傳情形
2.偵測能力	2.1 網路攻防演練驗證	2.1.1 以機關網路攻防演練狀況，評估 SOC 業者偵測能力
	2.2 國家資通安全研究院資安警訊驗證	2.2.1 以機關被通知之資安警訊，評估 SOC 業者偵測能力
	2.3 機關通報資安事件驗證	2.3.1 以機關主動通報之資安事件，評估 SOC 業者偵測能力
3.情資品質	3.1 資安監控情資品質分析	3.1.1 依據 SOC 業者回傳之資安監控情資評估內容正確性

		3.1.2 依據 SOC 業者回傳之資安監控情資之有效情資回傳率
		3.1.3 依據 SOC 業者回傳之情資分析單，評估是否有萃取分析之指標情資，包含受駭偵測指標(IOC)、攻擊指標(IOA)
	3.2 資安監控情資回饋能量	3.2.1 評估 SOC 業者回傳之資安監控情資有無額外回饋資訊，包含網際攻擊狙殺鍊分類資訊(Cyber Kill Chain, CKC)、MITRE ATT&CK、駭客工具與威脅手法分析情資、跨機關關聯性事件情資或重大資安弱點資訊等
		3.2.2 依據 SOC 業者回傳之資安監控情資之 ATT&CK 威脅樣態(Technique)資訊，評估其涵蓋率(ATT&CK 官網最新公告之威脅樣態資訊為準)
		3.2.3 依據 SOC 業者回傳之資安監控情資之情資調查率

資料來源：本院整理

4. 附件

附件1 監控設備狀況單格式範例

機關 OID 代碼	機關 名稱	責任等級	設備名稱與型號	設備代號	資安防護類型	觸發 次數	備註
機關_1_OID	機關_1	機關_1_等級	PaloAlto PA-3020	NICS_PaloAlto_1	網路防火牆	0	設備下線
機關_1_OID	機關_1	機關_1_等級	PaloAlto PA-3020	NICS_PaloAlto_2	網路防火牆	50	
機關_1_OID	機關_1	機關_1_等級	SonicALL NSA240	NICS_SonicAll_1	入侵偵測及防禦機制	100	
機關_1_OID	機關_1	機關_1_等級	TrendMicro Endpoint Sensor	NICS_TMES_1	端點偵測及應變機制	1	

補充說明：

1. 編碼語言請設定為 UTF-8。
2. 以 CSV 格式進行回傳。

附件2 資安情資回傳連通測試申請單

國家資通安全研究院
資安情資回傳連通測試申請單

以下方框欄位請以☑勾選

申請機關／單位			
用戶類型	□自行監控 □資安託管服務供應商	申請日期：＿＿＿年＿＿月＿＿日	
申請單位		機關 OID 編號： （無 OID 者不需填寫）	
地址：□□□　（縣市）　（鄉鎮市區）　（路街）　段　巷　弄　號　樓之			
申請人	姓名： 傳真：(　)	部門/職稱： E-mail：	電話：(　)　分機
主要聯絡人	姓名： 傳真：(　)	部門/職稱： E-mail：	電話：(　)　分機
次要聯絡人	姓名： 傳真：(　)	部門/職稱： E-mail:	電話：(　)　分機
請確認下列事項：			
□	（一）測試範圍：資通安全防護、目錄服務系統及核心資通系統		
□	（二）測試範圍：端點偵測及應變機制		
	（三）連通測試 IP：		
申請機關/單位印信			

申請機關/單位必須郵寄、電子郵件或傳真至下列聯絡方式進行書面申請。

聯絡地址：100057 臺北市中正區延平南路 143 號　聯防監控收

傳真：02-2733-1655　聯防監控收

電子信箱：ai2@nics.nat.gov.tw

服務專線：02-2739-1000

蒐集個人資料告知事項暨個人資料提供同意書

國家資通安全研究院(下稱本院)辦理「政府領域聯防監控資安情資回傳連通測試申請」(下稱本活動/業務)，向活動/業務參與者本人(以下稱「活動/業務參與者」)，蒐集下述個人資料，做為本活動/業務期間，活動/業務參與者身分確認、活動/業務相關訊息聯繫及本院辦理之活動/業務聯繫使用。為遵守個人資料保護法令及本院個人資料保護政策、規章，確保參與本活動/業務參與者個人隱私資料保護與權益，於向活動/業務參與者蒐集個人資料前，依法告知下列事項，敬請詳閱。

一、 蒐集目的及類別

(一) 目的：本院因辦理本活動/業務，基於活動/業務參與者管理、報名管理、活動/業務期間身分確認、活動/業務聯繫、相關行政作業及本活動/業務之驗收與稽核目的，須以電子或紙本方式獲取活動/業務參與者的下列個人資料類別。

(二) 資料類別：姓名、聯絡方式(如公務(行動)電話號碼、職稱、電子信箱或工作地址等)，或其他得以直接或間接識別活動/業務參與者之個人資料。

前述資料依據活動/業務實際蒐集項目為主。

二、 個人資料處理、利用之期間、地區、對象及方式

(一) 期間：蒐集目的存續期間(最長不超過活動/業務結束後 18 個月)及依法令規定應為保存之期間。

(二) 地區：中華民國境內。

(三) 對象：數位發展部資通安全署、國家資通安全研究院、依法有調查權機關。

(四) 方式：自動化機器或其他非自動化之方式。

三、 不提供個人資料之權益影響

若活動/業務參與者未提供正確或不提供個人資料，本院將無法為活動/業務參與者提供蒐集目的之相關服務。

四、 當事人權利

活動/業務參與者可依前述活動/業務所定規則或至本院網站之意見信箱(http://www.nics.nat.gov.tw/MailToCenter?lang=zh)向本院行使下列權利，惟因行使下列第(四)、(五)項權利，而致活動/業務參與者之權益受損時，本院將不負相關賠償責任。

(一)查詢或請求閱覽。

(二)請求製給複製本。

(三)請求補充或更正。

(四)請求停止蒐集、處理及利用。

(五)請求刪除個人資料。

五、 活動/業務參與者瞭解此一同意書符合個人資料保護法及相關法規之要求，且同意本院留存此同意書，供日後取出查驗，留存期限同第二條第(一)項。

六、 凡因本同意書而生之爭議，雙方以中華民國法律為準據法，並以臺灣臺北地方法院為第一審管轄法院。

個人資料之同意提供：

一、 立同意書人(活動/業務參與者)確認本人均已充分獲知且已瞭解上述貴院告知事項。

二、 立同意書人(活動/業務參與者)本人均同意貴院於所列蒐集目的之必要範圍內，蒐集、處理及利用本人之個人資料。

□立同意書人(已滿 20 歲)簽名：

□立同意書人(未滿 20 歲)簽名：

立同意書人之法定代理人簽名：

中　　華　　民　　國　　年　　月　　日

附件3連通測試檢驗單

國家資通安全研究院

連通測試檢驗單

測試單位(回傳單位)：_____

測試機關 OID：_____

測試 IP：_____

測試時間起迄：_____

項次	測試項目	Check (OK/Fail)	備註
1	情資單是否回傳成功		
2	情資單格式是否正確		
3	回傳情資類別 – 惡意內容		
4	回傳情資類別 – 惡意程式		
5	回傳情資類別 – 資訊蒐集		
6	回傳情資類別 – 入侵嘗試		
7	回傳情資類別 – 入侵攻擊		
8	回傳情資類別 – 服務阻斷		
9	回傳情資類別 – 資訊內容安全		
10	回傳情資類別 – 詐欺攻擊		
11	回傳情資類別 – 系統弱點		
12	回傳情資類別 – 其他		
13	資通安全防護 – 防毒軟體		
14	資通安全防護 – 電子郵件過濾機制		
15	資通安全防護 – 網路防火牆		
16	資通安全防護 – 應用程式防火牆		
17	資通安全防護 – 入侵偵測及防禦機制		
18	資通安全防護 – 進階持續性威脅攻擊防禦措施		
19	端點偵測及應變機制		
20	目錄服務系統		
21	核心資通系統		

測試結果: □通過 □未通過

測試員：_____

日　期：_____