## ● 立法院「資通安全管理中心」簡介

壹、 前言

立法院在資訊安全方面所面臨的挑戰很多，包括政治生態敏感、各類人員進出頻繁、機敏資料種類繁多、使用者意見多元、助理人員更換頻繁等，因此如何有效確保使用者資訊之安全，提供立法委員安全的問政資訊環境，是本院重要考量的議題。有鑑於此，本院於 2007 年 1 月依據國家資訊安全政策建立資通安全管理中心(Security Operation Center, SOC)，提供 7*24 小時全天候資訊安全監控服務，就各資安系統、主機系統(含各資訊應用系統)、網路系統、環控系統等進行監控，對資安事件進行發生前之偵測、早期預警通知、弱點補強、事件分析及鑑別與追蹤監控，並針對入侵事件進行通報及緊急應變處理，達到資通安全防範目標。

貳、 系統運作架構與功能

本院 SOC 運作架構如圖 1，說明如下：

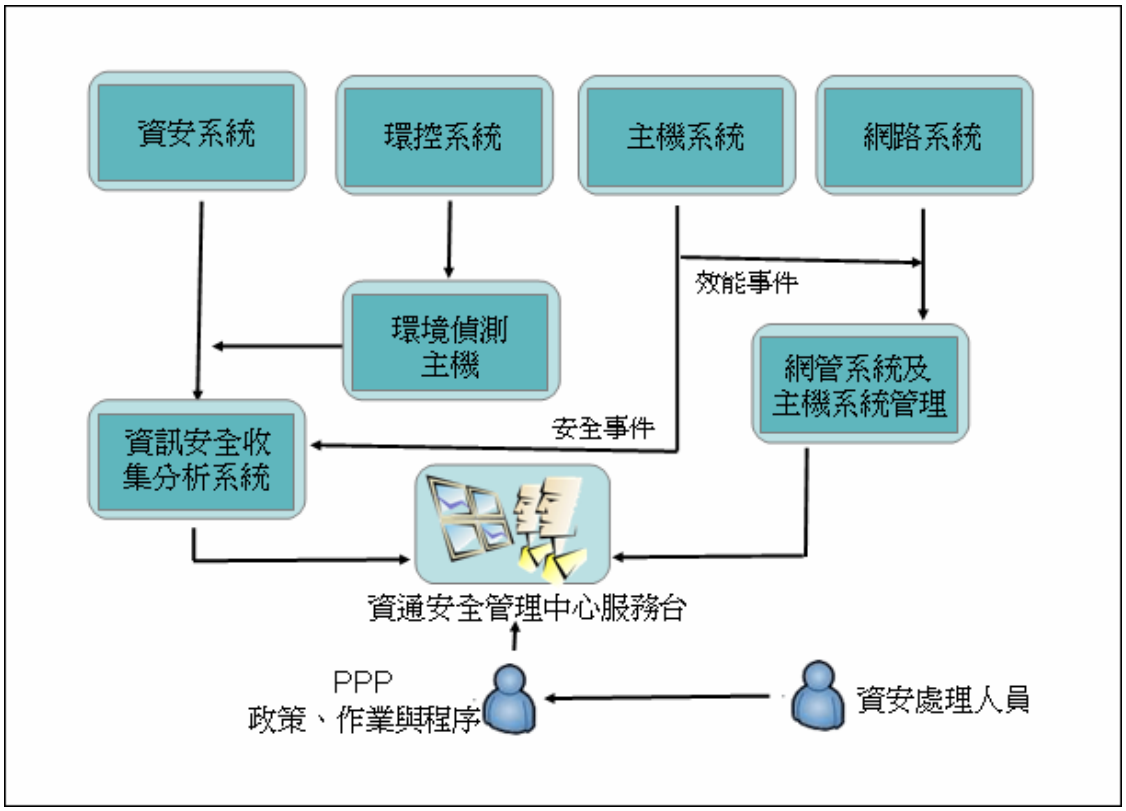


圖 1　SOC 運作架構圖

SOC 運作架構主要以資安系統、環控系統、主機系統、網路系統爲主，結合 SOC 服務台進行作業管理，SOC 服務台負責監控資安狀況，並依據資安政策、作業與程序(PPP)進行資安事件通報處理。

一、資安系統

SOC 收錄各資安設備之紀錄，包括防火牆、DNS、IPS/IDS 及防毒系統之紀錄，由資安人員全天候一天三班輪流監看資安事件，遇可疑事件時，可透過資安事件平台，進行資安可疑事件分析處理，並通報相關人員。另每天彙整分析提供

連結可疑中繼站 IP 及 DN 網域之報表，供相關人員至現場處理。

SOC 監控台人員，除了即時監控上述不同類型資安設備之紀錄外，另透過資訊安全收集分析系統設定之關聯規則監看資安事件，該系統可讀取各種資安軟硬體系統之日誌資料，經由解讀轉譯，轉換成各種不同的事件，再依據各資安事件之相互關連，進行分析並通報處理。

二、環控系統

本院為監控各資訊機房之溫濕度等相關資料，於各資訊機房安裝感應器，並將感應器相關訊息傳送至環控系統，可監控各資訊機房之溫度異常、濕度異常、空調異常、UPS 異常、火警警報、液漏警報、玻璃震碎警報等事件。環控系統之偵測主機接收不同機房之感應器資料，在主機中產生系統日誌檔案，並傳送至 SOC 進行事件的監控，另在 SOC 系統設定與機房環境有關之事件相互關係，並產生各種不同嚴重等級之意外事件，傳送至 SOC 監控台供監控人員即時處理。

三、主機系統

主機系統之事件，包括安全事件及效能事件。安全事件包括主機系統服務中斷或其他資安事件，會主動傳送訊息至資訊安全收集分析系統，並依據設定之規則，分析相關事件並監控管理。主機系統之效能事件，包括 CPU 使用率超過 80%、記憶體使用率超過 80%，硬碟容量空間使用率超過 85%等，另針對重要應用系統之可用性進行監控，各相關訊息會傳送至主機管理系統進行事件監控。若有主機系統之安全事件與效能事件時，會自動將意外事件訊息傳送到 SOC 監控服務台進行管理。

四、網路系統

本院 SOC 使用網管系統進行網路系統之監控作業，包括網路可用性及網路流量監控，會將網路相關資料傳送至網管系統中，並與主機系統之安全事件與效能事件進行整合，遇有網路中斷或網路流量過高之重大意外事件時，會傳送訊息至 SOC 監控服務台。

參、 資安事件通報處理及實施績效

本院已訂定資訊安全事件管理作業原則，當資訊系統及網路系統遭受破壞或不當使用等資通安全事件發生時，可迅速依通報程序進行通報，以加強處理效益及時程掌控，降低該事件可能帶來之損害，相關資訊安全事件處置流程如圖 2，說明如下：

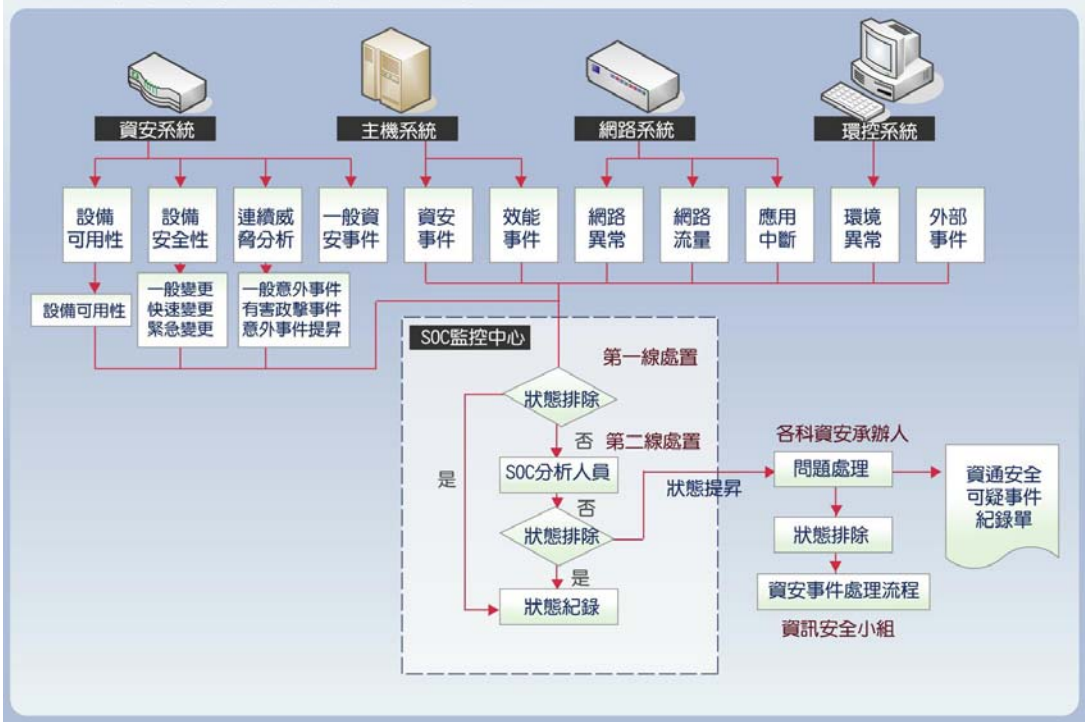


圖 2　資訊安全事件處置流程

本院 SOC 會收集資安系統、主機系統、網路系統、環控系統之相關事件，由 SOC 值班人員進行第一線處置，若狀況無法排除時，會經由 SOC 第二線分析人員進行資通安全可疑事件之分析，並依據本院資通安全事件處理通報流程，向各資安小組成員進行通報，各業務承辦人接到通報後，需考量該事件之影響範圍並依各系統之重要等級於規定時間內進行處理並紀錄。紀錄應分析資安事件影響程度、通報反映時間、問題處理完成時間，並定期將資安事件統計及通報事件提報資安小組覆核，以量化方式紀錄資通安全事件發生的頻率、程度、事件通報的成長率或問題處理完成時間，以達資通安全事件發生頻率、影響範圍的減低。

本院之資安事件認定原則如下：

A：本院同一網段總台數超過 1/3 台或同一網段發生 50 台以上電腦病毒感染。

B：伺服主機發生入侵或中毒事件。

C：範圍大或第一等級系統之中斷事件時間超過 1 小時以上。

D：範圍小、局部系統之中斷事件時間 4 小時以上。

E：範圍小、局部系統之短時間中斷事件每月發生次數 3 次以上。

F：機密性價值為 5，當資料外洩將導致個人權益嚴重受損。

G：資訊資產遭受未經授權的破壞或設定被竄改，影響二個以上系統業務運作。

H：其他重要資安事件。

若發生資訊安全事件後判定在資安事件影響等級 3 級（依據國家資通安全會報資安事件影響等級，等級 3 級：包括密級或敏感公務資料遭洩漏、核心業務系統或資料遭嚴重竄改、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）以上時，應依據本院資訊系統營運持續作業原則，啓動災害復

原管理機制。若經資訊安全工作小組認定屬重大資通安全事件需通報國家資通安全應變中心列管，由資通安全會報陳報召集人核可後方可通報，處理完成後結案。

本院 SOC 於 99 年 12 月通過資訊技術服務管理 ISO20000 認證，驗證範圍包括資通安全管理中心監控小組所提供服務櫃台、主機監控服務、應用系統監控服務、資訊安全監控服務、網路設備監控服務、機房環控監控服務及服務報告等服務。

本院 SOC 建置前，資安事件數量太大，難以判斷事件真假，造成誤報事件多，不僅耗時且耗人力，且各項資安設備之日誌記錄，由各負責人檢閱，資訊難以統合。SOC 建置後，監控人員容易發現可疑行為，誤報事件大幅降低，第一線人員不再疲於奔命，且統合各項不同設備之日誌，易於在事件發生時，迅速判斷問題點所在。本院 SOC 建置前資安事件數量平均每 30 秒有 18000 筆，建置後經正規化過濾後減少到每 30 秒約 400 筆，而監控人員檢視畫面的事件數量為 15 分鐘約 20 筆，其餘事件已根據過去的資料分類過濾，遇有新的攻擊事件或是已分類為攻擊之事件，會自動顯示於螢幕上，對於提昇本院之資訊安全幫助甚大。

肆、結語

本院近年來積極建立資安防護網，從監控面、流程面與管理面著手，舉凡資安事件發生前的防範－憑證管理中心、資通安全管理中心等監控管理，到事件發生時危機處理－資訊安全管理系統之緊急應變與處理能力，充分發揮標準作業流程效益，及事件發生後立即恢復正常營運－資訊系統異地備援中心等，嚴密的資安防護網，已有效阻擋駭客入侵或病毒感染，確保本院使用者資訊之安全。

（本文由立法院資訊處系統分析師吳天清　提供）