立法院資訊系統異地備援中心簡介

壹、前言

有鑑於美國 911 事件，兩棟超高大樓所有電腦資訊瞬間消失；回想臺灣發生的 921 地震，以及高雄、竹科大停電等天災人禍對台灣相關產業之影響深遠，如何作到不停頓的資訊服務及全面考量無預警的災害發生，降低運作風險所帶來的衝擊，是整體資訊安全管理最重要的一環，身為資訊技術(IT)人員自當從備援機制著手，考量電腦資訊之異地儲份、災害復原作業程序與執行速度等多方面實體技術建立；本院資訊系統異地備援中心於 93 年 1 月進行規劃建置，期間完成本院應用系統衝擊等級分析，依等級導入備份備援系統。異地備援中心於 94 年 1 月完成並正式啟用，94 年至 95 年間進行 3 次緊急應變實地演練，以期院區資訊中心系統因故障或天災導致運作停止時，可即時由異地備援中心備援機制接替，期使資訊應用服務不中斷；依據本院資訊系統風險等級需求及結合本院異地備援中心之大型主機、備援系統、儲存系統及高速傳輸網路等，可充分滿足本院國家級資訊安全目標需求。

貳、異地備援中心機房環境

一、 機房內均使用防火材料施工，辦公區域以矽酸鈣板耐火材、鋼絲網玻璃作為隔間，維運作業人員於辦公區域內可監視各區域與各資訊系統狀況，不會受到設備集中區域系統運作聲響干擾。

二、 機房大門輔助以鋼絲網玻璃自動門，配合監視系統及門禁管制設備有效紀錄與管控人員進出。

三、 地板建置以提供合金鋼 600 型高強度、高耐磨、承載力強之高架地板。

四、 消防系統並加裝極早期偵煙警示系統，於重要地點亦設置手提式填充滅火器，供災難發生時即時噴灑搶救。

五、 供電穩定度方面：使用二級供電保護措施，可滿足異地備援中心機房之用電需求。

(一) 第一級保護：設置 2 套 60KVA 的不斷電系統(UPS) 供應機房內資訊設備及空調用電使用。UPS 進向配電除市電外並由大樓發電機供電，若台電供電發生斷電情形，大樓的發電機會立即啟動接續供應電力給必要用電設施。

(二) 第二級保護：若發電機失效，UPS 配置之多組電池可於滿載情況下，由 UPS 迴路獨立供給異地備援中心機房連續使用 3 小時以上之電力。

六、資訊安全維運中心

(一) 機房環境監測 (冷氣空調、機房門禁、監控錄影、溫溼度控制及定址式液漏偵測等系統)。

(二) 網路安全管理。

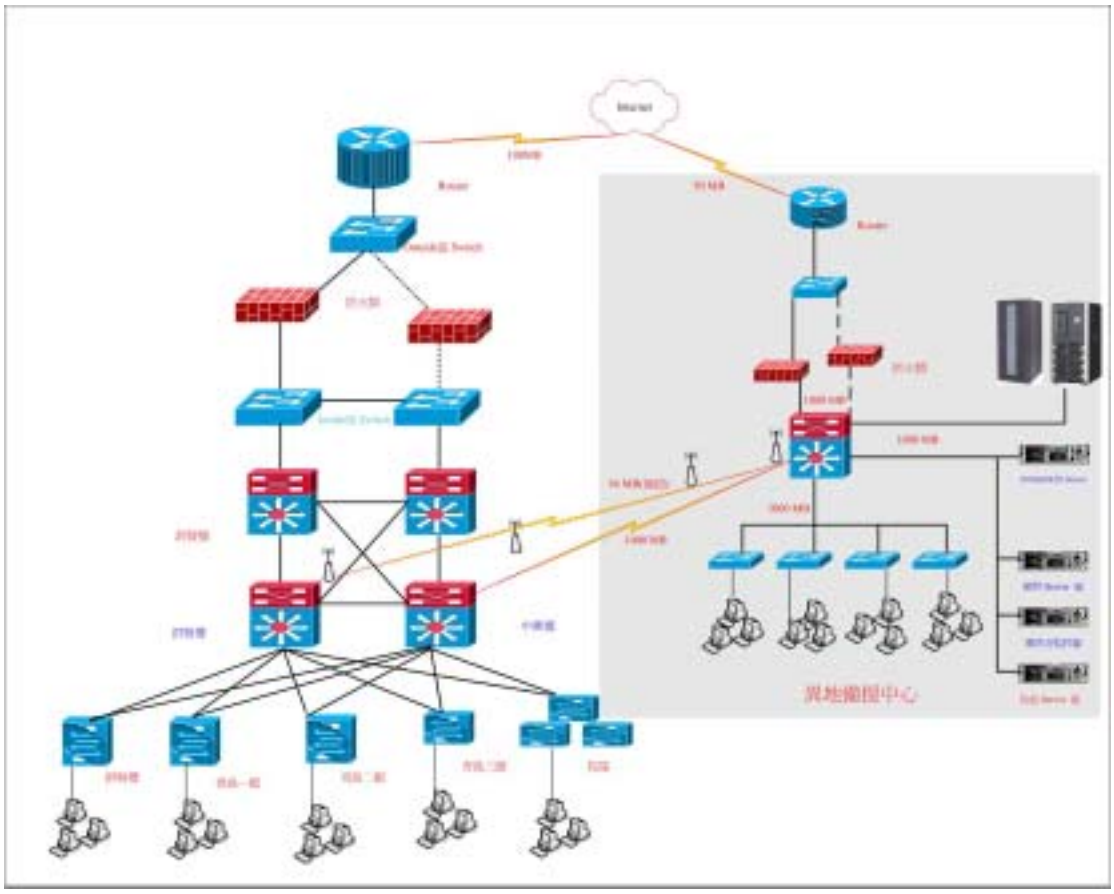
(三) 緊急應變集中控管能力。

參、異地備援中心網路環境

一、院區資訊中心機房與異地備援中心機房間以實體 1Gbps 寬頻網路連線(由固網業者提供雙迴路由異地端連接本院中興大樓)，並以無線傳輸 54Mbps 頻寬建立備援線路；以及備援機房至 GSN 網路 50Mbps 頻寬之連外線路(也可當作實體 1Gbps 寬頻網路第三備援線路)，以上三條線路皆建立 VPN 通道以防止本院與異地備援中心網路傳輸資料被竊取（圖一）。

二、備援機房至 GSN 網路 50Mbps 頻寬之連外線路亦可成為本院院區的對外連線備援線路，院區連接 Internet 之對外線路如果發生故障，可以經由手動修改路由設定，使院區使用者改由異地備援中心對外 50Mbps 頻寬連上 Internet 。

三、異地備援中心建置防火牆、DNS（網域名稱伺服器）、DHCP（動態分配 IP 伺服器）及防毒等系統服務，提供該中心完整之網路安全及傳輸服務。



圖一 異地備援中心網路架構圖

肆、資訊資產衝擊等級分析

一、資訊資產風險評估與衝擊影響等級評估

利用以下評估因子決定資訊資產衝擊等級：

(一)鑑別弱點

說明：利用弱點等級來鑑別資產的弱點等級

弱 點 鑑 別		等級評分	弱 點 鑑 別		等級評分
網路面	單一對外網路連接點		存放場所面	老舊的線路設計	
資料應用面	備份磁帶未能異地保管			資料中心未受限制存取	
	系統重要文件未能妥善保存			消防設施不夠完善	
	個人(筆記型)電腦資料未定期備份			建築物容易淹水	
	程式設計上的錯誤			缺乏整體環境控管機制	
	系統程式所使用函數之漏洞		系統設備面	所有資訊設備均存放同一地點	
	系統認證上的缺陷(密碼未妥善管制、不當授權)			設備零件容易故障	
	未能妥善處理系統例外錯誤產生			零件過期或缺少替代品	
	未完善使用防毒軟體(未安裝、過期)			系統軟體升級未經完整測試	
使用者	教育訓練不足			電力不穩定(電力中斷、突波、電壓下降)	
	螢幕未淨空				

(二)鑑別威脅

說明：利用威脅等級來鑑別資產的威脅等級

人為因素之威脅		發生率(%)	自然因素之威脅		發生率(%)
蓄意性	駭客攻擊		大自然力量	暴風雨(例如：颱風)	
	病毒、蠕蟲與木馬程式威脅			火災/濃煙	
	阻絕服務攻擊漏洞(D.O.S.)			水災	
	炸彈攻擊			地震	
	強盜/竊取			濕氣	
	人為勾結或政治上間諜		設備/設施故障	公共設施故障(電力、電訊)	
	惡意破壞(系統、設備、機房)			硬體主機故障	
	垃圾電子郵件			系統軟體失效	
非蓄意性	資訊安全意識不足			建築物結構上的缺陷	
	不安全的行為(例如：未遵守標準作業程序、人員操作疏失)				

(三)鑑別資產等級

1、資料回復點(RPO,Recovery Point Objective)：備援中心取代原有資訊中心時，在資料上所能回復的時點(可以承受在某一段時間內所遭受之資料損失)

2、系統恢復時間(RTO,Recovery Time Objective)：備援中心取代原有資訊中心提供服務所需的回復時間(可以承受之營運中斷時間)

二、資訊資產衝擊等級備援備份說明：

(一)第 1 級：異地備援

本院院區資訊中心與異地備援中心都處於正常運作狀態，進行相互資料備份，出現災難時，可迅速將資訊系統切換至異地端，接替本地系統正常運作，確保業務的持續性。

(二)第 2 級：異地資料備份

在異地備援中心建立一個備份系統，透過網路進行資料備份。也就是透過網路以同步或非同步方式，把本院資訊中心的資料備份到異地備援中心的備份系統上，備份系統一般只備份資料，不負責系統運作。

(三)第 3 級：本地資料備份，異地保存

在本院資訊中心將關鍵資料備份，然後將送到異地保存。災難發生後，按預定資料恢復程序進行系統和資料的回復，此組備份作業本院目前由 1Gbps 寬頻網路直接備份至異地備援中心儲存。

(四)第 4 級：本地資料備份，不異地保存

只在本地進行資料備份，並且被備份的資料只在本地保存，沒有送往異地。

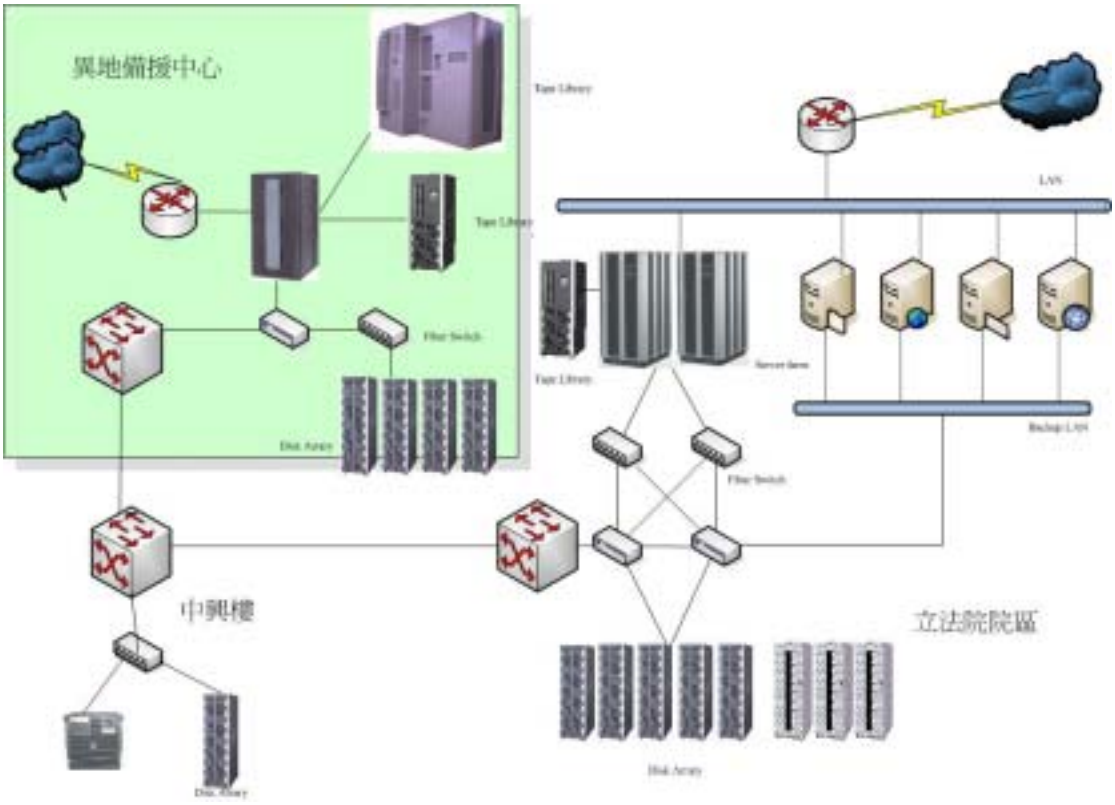
伍、主機資料備份及異地備援機制介紹

一、本院備援主機系統配合本院各應用系統備援需求，共分成十一個系統分區。

二、資料備份主要採用備份軟體系統搭配磁帶館作各應用系統資料備份及資料庫備份；有關大型主機資料備份部分除了使用以上備份機制並行採用 TimeMark 技術作資料快速回復機制。

三、異地備援機制則採用 Replication 作法，定時將本地端資料複寫至異地備援中心存放，待災難發生或需啟動異地備援機制可隨時接替院內重要系統運作；院內儲存設備利用 Mirror 至本院中興大樓儲存設備達到主機資料存取不中斷服務（圖二）。

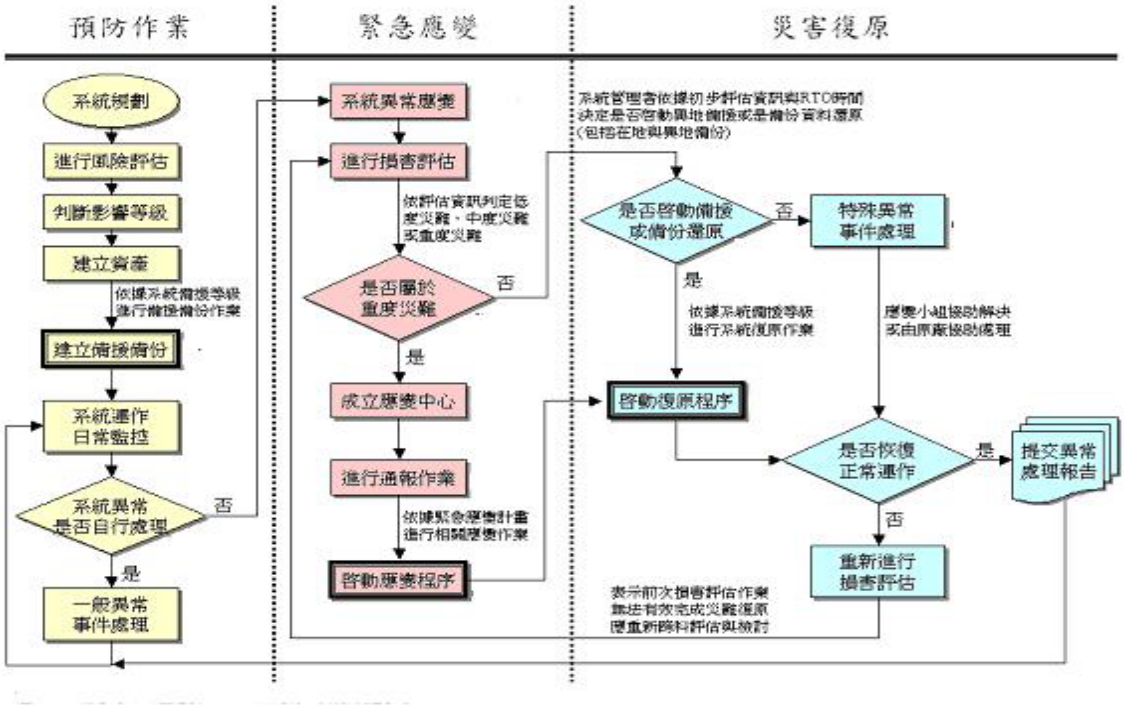
四、異地備援中心亦建置一套備份軟體系統與磁帶館，將院內資料作異地存放及備份。



圖二 異地備援中心備份備援機制

陸、資訊系統緊急應變作業

一、緊急應變運作流程



(一)預防作業

預防作業之主要目的在於日常之備援備份作業，並提供系統運作之日常監控。

(二)緊急應變

本階段之重點在於系統異常狀況發生後之應變作業，並採取損害評估作業程序，確保應變作業順利進行。

(三)災難復原

該階段為系統發生重度災難或特殊異常狀況時，進行系統復原作業，以確保系統的持續運作。

二、考量本院資訊安全重要性暨配合本院資訊安全管理系統（ISMS）「災害復原管理作業原則」之要求，執行每年兩次演練計畫，本處動員相關人員以進行資訊系統災害復原標準作業程序（SOP）及緊急動員演練作業，演練作業旨在提升資訊人員在面臨各種突發狀況時之通報與應變能力，以滿足緊急應變實際作業需求。

柒、結論與展望

本院為配合國家資安政策推動，全面發展資訊系統備援服務與應變措施作業機制，俾使本院於未來各項資訊通訊與應用服務，均能確保其永續運作與資料完整，建立更優質安全之國會資訊環境。

（本文由立法院資訊助理管理師曹志強 提供）