論述 》管理 · 資訊

疫情期間彈性辦公規劃　強化組織韌性眞便利

為配合防疫政策，各級政府皆須採取相關防疫提升作為及啓動相關應變措施，本文就行政院主計總處疫情期間彈性辦公規劃及辦理情形予以簡要說明，以供各界參考。

賴柏宇（行政院主計總處主計資訊處分析師）

壹、前言

病毒不斷在變異，疫情也一直變化，110 年我國面臨首波本土嚴重特殊傳染性肺炎（以下簡稱 COVID-19）疫情大規模爆發，並於當年 5 月進入第三級警戒，各級政府除了須配合防疫政策，採取相關防疫提升作爲外，爲照顧民衆需求，更須提出各項防疫、紓困、振興等因應措施。行政院主計總處（以下簡稱本總處）職司政府預算分配、會計處理及統計調查等工作，雖非第一線防疫機關，但舉凡政府各種施政措施都需要預算支持，本總處業務必須能持續營運以作爲政府對抗疫情的堅實後盾。

因此，自 109 年初疫情開始發展時，本總處已著手啓動各項部署，包括規劃彈性辦公及相關演練，並據以發展業務營運持續計畫；同時，亦積極備妥各項「數位防疫物資」，以確保彈性辦公措施啓動時，本總處各同仁都能順利處理公務，以強化組織持續營運之韌性。

貳、彈性辦公規劃及辦理方式

一、數位環境整備

所謂工欲善其事，必先利其器。重要物資之整備及掌控實爲首要之務，就如同防疫時期疫情指揮中心對於口罩、疫苗、快篩試劑等「防疫物資」的管控，本總處亦早於疫情發生之初即整備所需「數位防疫物資」，以因應疫情變化發展，重點分述如下：

（一）盤點關鍵物資：包括網

路交換器、遠端安全存取設備（即 SSL VPN 設備）、筆記型電腦、備用電腦、讀卡機、延長線、印表機驅動程式等資訊軟硬體資產，並將相關設備物資編號造冊。由於掌握資產現況，得以儘早採購所需物資；相關資源亦統籌調配控管，並記錄分配使用情形，掌握物資動向。

（二）快速採購所需物資：如讀卡機、延長線、無線網卡、USB 外接擴充集線　器（USB HUB）、視訊會議設備組（包含視訊鏡頭、耳機、麥克風）、視訊會議軟體及 SSL VPN 系統授權等。此外，對於預計汰換之個人電腦，協調各使用單位（人員）改採筆記型電腦辦理汰換，以便快速部署建置視訊會議及居家辦公環境。

二、發展業務營運持續計畫

無論是分區辦公或居家辦公，本總處在疫情之前並未試辦過混合辦公型態。因此，除了須要驗證技術可行性，尚須發展一系列之營運持續計畫。於 109 年我國尚未爆發本土疫情時，本總處即辦理居家辦公測試作業，並試辦分區辦公，已奠定強化組織韌性之良好基礎：

（一）請各單位同仁實地演練居家辦公及試辦分區辦公，以發掘日常辦公時實際面臨之情境與問題。根據演練結果，完成制訂「行政院主計總處因應嚴重特殊傳染性肺炎居家辦公工作規範」、「行政院主計總處居家辦公資訊服務作業原則」及「遠距辦公資訊安全防護作業說明書」等規範及相關服務申請流程、表單。

（二）製作資訊服務便利包，整合居家及分區辦公所需流程指引、申請文件、硬體設備借用、軟體安裝及設定、服務使用說明以及障礙排除手冊 FAQ 等，透過居家辦公資訊服務便利包（下頁圖 1），協助本總處同仁能快速取得所需資訊及服務，得以彈性辦公模式便利地處理業務。

三、彈性辦公資訊安全防護

根據「趨勢科技 2021 年度網路資安報告」，駭客持續提高針對企業和個人的攻擊頻率，整個 110 年（2021 年）所偵測到的全球勒索攻擊數量，臺灣位列全球前十名、亞洲區前五名，而政府機構、銀行與醫療產業是當年最常遭受勒索攻擊的前三大產業。由此可見，網路駭客或惡意行為非但未受疫情影響，反而更為猖獗。因此，實施彈性辦公時亦須考量資安防護：

（一）分區辦公安全

本總處於 105 年時，內部網路環境就已完成網路存取控制（Network Access Control，以下簡稱 NAC）架構建置[1]，在此架構下，經

論述 》管理 · 資訊

存取授權的使用者設備（如電腦、筆電或印表機）在本總處內部任何地點，只要接上網路就能上網；反之，未經授權的設備即便接上網路亦無法使用，兼顧網路使用方便性及資安考量。就好像國外來的旅客要入境時，要先過海關驗明正身，持有合法授權才可以通行。此外，NAC 網路環境讓同仁電腦（或印表機）於本總處各區域都能使用相同的網路位址（IP Address）上網無須另行設定，爰於分區辦公正式實施時，協助同仁快速進入分區後的辦公環境，減少額外設定成本，順利業務接軌運作。

（二）居家（遠距）辦公安全

根據原行政院資通安全處（現爲數位發展部資通安全署）於 109 年發布之相關規定，個人資通訊設備不得處理公務事務，亦不得與公務環境介接。爰此，本總處訂有「行政院主計總處居家辦公資訊服務作業原則」，規範以使用本總處配發之公務用個人電腦、筆記型電腦處理公務爲原則；如經核准使用自備電腦，則須以透過虛擬桌面（Virtual Desktop Infrastructure，VDI）[2] 存取公務電腦桌面環境之方式辦理。

因應遠距辦公需求，提供資訊服務檢核表（下頁圖 2）供居家同仁參考相關流程步驟，並能自我檢核設備狀態。其中，設備於外部網路環境（例如居家或出差）必須使用安全的遠端連線措施（即 SSL VPN）與本總處內部網路建立連線，以保護內部的資料與系統存取安全。VDI 及 SSL VPN 適用情境說明如下頁圖 3。

爲便利管理及使用，本總處將 SSL VPN 帳號驗證與辦公室電腦登入帳號結合綁定，同仁無須再記憶額外的帳號、密碼。除了使用帳號、

圖 1　本總處居家辦公資訊服務便利包

資料來源：行政院主計總處知識管理平臺。

密碼驗證身分，也再啓用雙因子驗證（2FA）功能[3]，結合手機認證提供多一層身分驗證保障。

（三）落實資訊安全管理

根據行政院公布之「110年國家資通安全情勢報告」，資安事件類型以「非法入侵」事件居多，主要肇因係使用弱密碼或者委外廠商維運管理疏失等，惡意攻擊者會尋找及測試機關資安防護最脆弱之一環（例如委外之資訊服務供應商），一旦攻擊成功即成爲跳板，進而展開進階或橫向擴散攻擊。因此，無論是否實施彈性辦公，平時即應重視資訊安全管理，持續加強各項資安防護策進作爲，尤其建議落實以下基本要求：

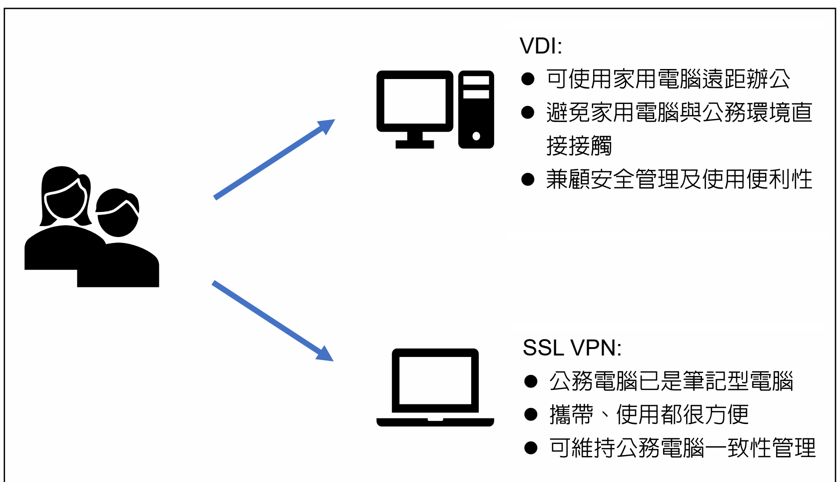
1. 依據最小權限原則設定所需權限：系統（或設備）在開發或測試時，往往爲了方便而開啓過大的權限，卻也經常因疏於管理而淪爲系統漏洞。爰此，針對資通系統使用者應給予最小且足夠的存取權限，對於特權帳號應定期清查並限縮使用方式（例如只能經由指定位址存取），無須再使用之帳號或功能應關閉。
2. 管理及定期追蹤軟硬體更新狀態：惡意攻擊者總是千方百計要找尋機關的漏洞，持續不斷的利用各種工具、手法進行探測。系統或設備管理者應注意行政院國家資通安全會報技術服務中心所發布的漏洞警訊公告，執行更新或其他修補措施，並定期追蹤更新或修補結果。

圖 2　本總處資訊服務檢核表

單位			姓名	
階段	項目	說明	檢視結果	備註
第1階段設備準備	1-1. 居家辦公資訊服務申請	□申請，填寫「101表_居家辦公資訊服務申請表」	□完成	以各單位依居家辦公名冊，統籌申請單，交由主計資訊處辦理
	1-2. 第二類資訊服務申請	□申請，填寫「102表_VPN網路申請表」	□完成 □不需要	以各單位依居家辦公名冊，統籌申請單，交由主計資訊處辦理
	1-3. 居家電腦設備	□配發個人電腦 □自備電腦 □配發筆記型電腦	□完成	自備電腦者免填1-7、3-1、3-2並請依[illegible]辦理。
	1-4. 備份資料	□自行備份重要資料 □下載「居家資訊服務便利包」	□完成 □完成	➢「KM首頁>防疫資訊服務專區」下載
	1-5. 各類資訊服務需填申請VPN	□安裝VPN □在辦公室測試VPN	□完成 □完成	➢執行安裝檔 FortiClientVPNOnlineInstaller_

資料來源：行政院主計總處知識管理平臺。

圖 3　VDI 及 SSL VPN 比較說明



資料來源：作者自行繪製。

論述 》管理 · 資訊

3. 開啓日誌保存功能：惡意攻擊者並非幽靈，來去仍有跡可循，惟若疏於記錄，則所有痕跡亦如歲月消逝於時光洪流中。依行政院「各機關資通安全事件通報及應變處理作業程序」，各機關於日常維運資通系統時，應依自身資通安全責任等級保存日誌（log），並建議定期備份至與原稽核系統不同之實體系統，所保存日誌（log）至少應包含：作業系統日誌（OS event log）、網站日誌（web log）、應用程式日誌（AP log）、登入日誌（logon log）等。

參、結語

COVID-19 疫情已肆虐全球近 3 年，社會各行各業均面臨業務持續營運的重大挑戰。爲對抗疫情帶來之衝擊，許多行業絞盡腦汁，紛紛力求轉型以求在這場抗疫戰爭中存活。我們也觀察到其中許多成功案例，例如傳統零售超市結合外送服務，在疫情催化下，反而帶動外送服務下需求攀升，迅速拓展了電商業務，展現出高度韌性。探究這些成功案例，善用數位科技及積極推動數位轉型實爲關鍵因素。

本總處爲全國最高主計機關，因應數位科技應用發展趨勢，亦不斷精進主計業務，例如近年來所推動之經費結報全程電子化，優化傳統紙本作業流程，其無紙化、零接觸等特性，即使面對疫情威脅，也能高效率的完成作業。展望未來，本總處將持續善用科技力量推動數位轉型，與全國主計人員一起努力，增強營運免疫力，提供更堅韌的數位服務。

註釋

1. 網路存取控制（NAC）架構能管理組織內部網路位址（IP Address）的使用，使用者設備的網路位址只能藉由統一派發方式取得，無法自行設定；針對未經授權之設備可以派發特定之網路位址，以限制其連網能力，確保資訊安全。
2. 虛擬桌面（VDI）是一種集中建立和管理電腦桌面的軟體工具，使用上近似於遠端桌面，提供使用者在組織外部可以透過網路連線使用辦公室內的電腦。
3. 所謂「雙因子驗證」方式，就是同時採用 2 種不同鑑別因子的驗證技術，目前鑑別因子分爲以下 3 類：「基於所知（something you Know）」，例如帳號密碼組合、「基於所有（something you Have）」，如透過簡訊發送的認證碼或晶片卡、「與生具備（something you Are）」，如指紋或臉部特徵。

參考文獻

1. 趨勢科技 2021 年度網路資安報告，https://www.trendmicro.com/zh_tw/security-intelligence/threat-report.html。
2. 行政院國家資通安全會報技術服務中心，VPN 安全參考指引，https://www.nccst.nat.gov.tw/CommonSpecification?lang=zh。
3. 數位發展部資通安全署，110 年國家資通安全情勢報告，https://moda.gov.tw/ACS/press/govinfo/report/1351。❖