

# 後疫情時代的 雲端資料 安全管理

／ 科技大學講師 魯明德

2020 年是企業對內部資訊管理的一個轉捩點，受到新冠病毒（COVID-19）疫情的影響，人們的工作模式也有了另類的思考。

## 疫情的衝擊

有些公司為了降低辦公室的人員密度，規劃輪流上班，甚至推動員工異地上班、在家上班等措施，以避免可能的感染對公司的營運造成衝擊；各級學校為了讓教學能順利進行，開始超前部署，規劃停課時的遠距教學方案。

但是，不論是異地上班、在家上班還是遠距教學，所要面臨的都是「從外部存取資料」的安全問題，因此，如何建置一個安全的系統，就成了當務之急。

## 雲端平台的趨勢

以往的觀念為了資訊的安全，最好是把所有的資料建在自己能控制的平台上，當面對異地存取資料的需求時，這個方法就面臨挑戰了。雲端運算（cloud computing）是近年新興的技術，使用者只要透過網路登入伺服器（server），就可以操作各項工作。而雲端平台的服務就是一個基礎建設，未來它就像水、電等公共系統一樣，只要接上就可以使用服務。



因應疫情衝擊，各公司、學校規劃在家上班、遠距教學等方案，均面臨從外部存取資料的安全問題，因此建置安全的系統成為了當務之急。



圖 1 雲端架構

(圖表內容：作者提供)

雲端安全聯盟 (Cloud Security Alliance, CSA) 針對雲端運算所面臨的資訊風險，提出建立雲端運算安全架構的方法，包括了雲端架構 (cloud architecture)、雲端治理 (governing in the cloud) 及雲端營運 (operating in the cloud) 層面。

在雲端治理方面，主要關注在以下 5 項資訊安全領域的問題：企業治理與風險管理、法律上的契約與電子證據、法規遵循與稽核管理、資訊管理與資訊安全、相互運作與可攜性。

而大多數使用者所關切的雲端營運在技術面上的安全議題不外乎是：業務持續與災害復原、資料中心營運、資安事件應

變、應用程式安全、加密與金鑰管理、權限識別與存取管理、虛擬化、安全即服務。

### 資料放到雲端是否安全？

雲端運算的概念已提出多年，相關的技術、服務均已趨成熟，然而，雲端運算仍是架構在既有的資訊科技 (information technology, IT) 之上，因此，傳統資訊系統所面臨的資訊安全議題，在雲端依然會出現。

企業導入雲端運算之後，在資訊管理上面對的問題，將會從企業內部延伸到利害關係人，資料放上雲端的目的是在共享，因此，存取的使用者變多，所衍生的資訊安全問題也變多。



圖 2 雲端資料存取方式

(圖片來源：作者提供)

雲端資料所產生的資訊安全風險可歸納為 3 方面：網路、資料安全、資料管理，網路風險可透過防火牆、實體隔離等技術予以解決，以下將探討資料安全與管理上的問題。

### 一、雲端資料安全

資料放上雲端，可方便利害關係人下載閱讀，如企業的產品或零件設計圖可以放在雲端，讓供應商可以直接下載，以評估內容進行報價。法院的訴訟資料，也可以放在雲端，讓兩造的律師自行下載，以減少人員奔波。

但是，資料的擁有者可能會擔心：雲端資料是不是會被不相干的人下載、閱讀、重

製、散布？當然，資料存在雲端，它占有一定的空間，既然占有空間，就不可能不被不相干的人看到，因此，在資訊安全上要做的不是不被看到，而是看到也看不懂。

當資料擁有者要將資料存放到雲端時，並不是存放明文 (plain text) 資料，而是存放一個經過加密後的檔案，明文資料經由一個加密函數以使用者的金鑰加密才能上傳，因此，雲端上存放的產品或零件圖、訴訟文件都是加密後的亂碼，不相干的人即使下載了也看不懂。

當利害關係人下載後，必須要有文件擁有者所給的解密金鑰及當初的加密函數，才能把所下載的資料打開，也就是說，

供應商從雲端下載了產品或零件圖，也同時會拿到解密金鑰；律師在接受委託、申請閱卷時，也會取得一個授權的解密金鑰，以便日後下載訴訟資料時可以閱讀。

文件的使用者在每次打開文件時，解密金鑰都會自動由金鑰伺服器確認有效期，因此，文件擁有者可以控制文件使用者的閱讀時間與權限，如報價期間如果設定為5天，則5天後供應商就打不開下載的零件圖了；同理，律師在解除委任關係後，金鑰伺服器就會停止金鑰的權限，其下載的檔案亦無法開啟。

## 二、雲端資料管理

在談資訊安全時，大家都會專注於外部的攻擊，所以要設防火牆、避免弱點被攻擊，但是，往往會忽略內部的合法使用者，

所謂外賊易擋、家賊難防，除了教育訓練、管理制度、定期稽核外，雲端資料除了要加密外，每一次的存取都要留下紀錄。

系統建置時，都會設置 log 檔，log 檔會記錄檔案每次存取的資料，如是誰在什麼時候存取了哪個檔案，系統可以定期把異常存取的資料列出，進行檢討、追蹤，可以提早發現問題，防範於未然。

## 結論

後疫情時代改變了人們的工作模式，資料放到雲端管理已經是未來的趨勢，對於資料放在未知的雲上，很多人都對其安全心存疑慮，然透過加密技術讓資料不被無關的人存取，並記錄每次存取的事件，將可提升使用者對雲端資料存取的信任度。



透過金鑰加密與解密，讓雲端資料的共用與存取更加安全，但除了重視外部攻擊，更別忽略內部的教育訓練、管理制度及定期稽核系統，否則易導致外賊易擋、家賊難防的窘境。

# 淺談資安風險管理： 以遠距視訊為例

／金門縣政府政風處專員 陳大中

資安風險管理為資安防護之基礎，唯有完善的風險管理，方能逐步建構更臻妥適之資通安全防護網。



## 全臺上網人數已突破 2 千萬

依據財團法人臺灣網路資訊中心「2019 臺灣網路報告」，推估民國（下略）108 年全國 12 歲以上曾上網人數達 1,898 萬人，而全國上網人數（包含未滿 12 歲）已達 2,020 萬，整體上網率高達 85.6%，為歷年最高<sup>1</sup>。換言之，我國各項資訊科技及

網際網路不僅日益普及，更有快速發展之趨勢。

## 公私部門因資安破口，遭受鉅大損害

然隨著網際網路及其他資通科技之迅速發展，亦帶來資訊安全危機，如：銓敘

<sup>1</sup> 109 年 7 月 3 日引用於財團法人臺灣網路資訊中心「2019 臺灣網路報告」，網址：[https://report.twnic.tw/2019/assets/download/TWNIC\\_TaiwanInternetReport\\_2019\\_CH.pdf](https://report.twnic.tw/2019/assets/download/TWNIC_TaiwanInternetReport_2019_CH.pdf)。



銓敘部

Ministry of Civil Service, Republic of China (Taiwan)

[回首頁](#) [部長信箱](#) [訂閱電子報](#) [English](#) 字級大小: [A-](#) [A](#) [A+](#)

查詢 進階查詢

熱門查詢: 年金改革, 退休金, 撫卹, 社團年資

[本部簡介](#) [公告資訊](#) [各司業務](#) [銓敘法規](#) [銓敘統計](#) [服務園地](#) [傑出貢獻獎](#)
目前位置: [首頁](#) > [公告資訊](#) > [新聞稿](#)
[f](#) [g+](#) [t](#) [p](#) | [友善列印](#)

## 銓敘部主動掌握歷史資料外洩 全面檢視資安防護

本部於108年6月22日接獲外部情資知悉國外網站揭露疑似本部所掌理之個人資料約59萬筆。該疑似外洩資料為本部94年1月1日至101年6月30日間中央及地方機關公務人員送審人員歷史資料，經比對後實際影響人數為24萬餘人。該外洩資料為善公文管理系統之收文資料，並非最新銓敘審定資料，且該系統已於104年3月即下架。

本部第一時間已依規定通報，並主動處理，同時全面檢視現行系統，有可疑的弱點均已補強，完成修補。本部並依個人資料保護法第12條及施行細則第22條規定通知當事人相關影響範圍及因應措施，同時於本部官網正式公告通知。

為確實強化本部各資訊系統之安全防護，已協請行政院資安處組成專案團隊協助，並進行實地查核，並就本次事件進行追緝。

後續本部亦將提昇資安防護作為，同時強化系統開發之安全管理及委外管理。(108-06-25)

銓敘部於108年6月公告接獲外部情資知悉國外網站揭露歷史個資，經確認後掌握外洩資料內容，並下架舊系統，補強現行系統之可疑弱點，全面檢視資安防護。(圖片來源：載自銓敘部官方網站，<https://www.mocs.gov.tw/pages/detail.aspx?Node=489&Page=6145&Index=0>)

將加密金鑰存放位於中國大陸的伺服器，有遭駭客竊聽之虞。隨後爆發英國金融時報記者藉由竊聽其他報社運用 Zoom 視訊軟體召開的會議，刺探其他報社之新聞訊息。不僅如此，香港中文大學使用 Zoom 視訊軟體進行遠距考試，系統被不明人士駭入，考試時透過該軟體分享個人電腦螢幕，播放色情成人片、舞曲 MV 等，Zoom 的各種資安事件接踵而來地發生。因此，電動車大廠特斯拉、美國國家航太總署及英國國防部等機構陸續宣布禁用 Zoom 軟體。

## 視訊軟體 Zoom 之資安隱憂

全球因受新冠病毒蔓延影響，遠距視訊軟體開始廣泛使用，其中 Zoom 視訊軟體資安疑慮遭連環踢爆，先是該視訊軟體

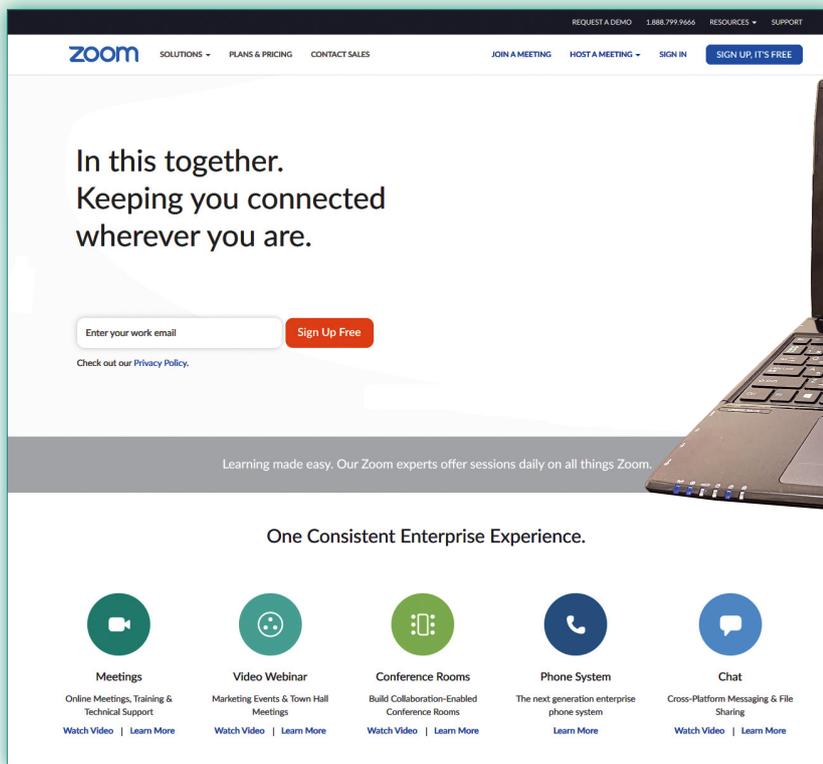
## 資安風險管理步驟

為免更多公、私部門或個人因資安破口，遭受鉅大損害，我國亟待正視資安防



107年台積電設備遭電腦病毒 WannaCry 感染，造成產線停擺，損失慘重。(圖片來源：載自中視新聞，<https://www.youtube.com/watch?v=D0ud9d6C2S0>)

部108年6月間經報導指出超過24萬筆個人資料遭外洩，台積電於107年8月初設備遭電腦病毒 WannaCry 感染，該次中毒事件影響台積電營收估計新臺幣25.96億元(依台積電107年第三季財報數據)，足堪為我國史上損失最大的資安事件。今年5月間不僅國內多家重要能源及科技公司接連遭勒索軟體攻擊，甚至爆發位列資通安全責任等級最高級A級之總統府電腦也遭駭客入侵事件。



受疫情影響，遠距視訊軟體開始廣泛使用，其中 Zoom 視訊軟體資安疑慮遭連環踢爆。  
( Photo Credit: Project Kei, [https://upload.wikimedia.org/wikipedia/commons/2/23/Video\\_Conference\\_Using\\_Laptop.jpg](https://upload.wikimedia.org/wikipedia/commons/2/23/Video_Conference_Using_Laptop.jpg) )

護問題，然資安防護沒有百分之百，不同資通環境，都存在不同的弱點與威脅，只有透過不斷精進，確實做好風險管理，才能將資安風險降到最低，因此，無論是公、私部門或個人，都應確實認識強化資安風險管理，管理步驟有四：

首先，應先識別風險，不論是公務機關、私人機構或個人，均應對其本身及所屬部門之資安風險全貌確實掌握，雖然各部門業務、作業差異甚鉅，可能潛存的風險因子不盡相同，然仍應審酌不同業務屬性，做出可識別的異質性資安風險因子，做好風險識別，是管理的基礎，也是最重要的一個步驟。

其次，進行風險評估，針對資訊資產可能存在的每個資安風險，逐一分析，分析要項包含評估曝險係數、發生可能性、發生時之影響程度、損失預期範圍及處理之優先順序等，確實風險分析與評估，以為後續有效之管理與因應。

第三，深入檢視風險成因，瞭解可能之外在威脅與本身潛存之弱點，透過確實認識可能造成資訊設備、系統危害或威脅之外在影響因素，如系統內容遭駭或遭植入惡意程式，致機密資料遭竊取、竄改，或造成原有之服務不得不中斷等；以及掌握資訊系統或資訊設備本身可能存在的弱點，例如硬體設計存有缺陷、無防火牆設

備、軟體測試不足、內部控制未確實等，唯有全方位檢視風險成因，清楚分辨外在可能危害之威脅與內在潛存之弱點，才能進行有效之相應安全管控或對策，避免損害發生或擴大。

第四，提出最適切之風險因應，當風險經識別出來及評估後，須提出相應之處理計畫，處理方式大致上可區分為避免風險、轉移風險、降低風險及接受風險。我們須先思考有無方式避免風險，如無法避免，退而考慮能否轉移風險，若無法避免又無法轉移，就審酌有沒有辦法降低風險

可能帶來的影響與衝擊，最後，如果無法處理或需處理成本過於巨大，接受風險，也算是一種選擇。

### 使用遠距軟體之風險管理

以遠距軟體為例，使用前應提前做好風險管理，其一，選購本身較無資安疑慮之產品，不論公、私部門在使用遠端視訊產品前，均應由資安管理單位或請專業之資安人員，協助全面盤點遠端視訊之同質性產品，了解產品是否符合《資通安全管理法》等相關規定，是否存有將資料回傳



圖 1 資安風險管理步驟

至特定地區之伺服器的疑慮，汰除有資安風險之產品，擇優選用符合規定之遠端視訊產品。

其二，進行遠端視訊會議或教學前，應修改密碼，避免使用弱密碼，更不得便宜行事，取消密碼。進行安全性及相關環境設定，落實人員管控，非屬該次會議或教學之第三人，未經同意，不得進入。

其三，針對遠端視訊產品之操作人員做好教育訓練，以利視訊之正常進行，遇有狀況，方得以迅速處置。

其四，凡機密、敏感議題或資料，均不宜於遠端視訊會議或教學使用，避免不慎洩漏，造成重大損害。透過完善資安防

護措施，減少外在威脅及內在弱點，讓風險因子降到最低，持續落實資安風險管理，讓遠距辦公或遠距教學，更加安心踏實。

## 資安即國安

資訊安全不僅是安全與便利的取捨，更關係整體國家安全與國家利益，近年政府為強化資安工作，陸續完成相關法制作業，然徒法不足以自行，若要達到有效資安防護，就須做好妥善之資安風險管理，並逐步落實資安環境的改善，減少風險的存在，並培養資通使用者之資安觀念及敏銳度，提升其資安防護之素養與能力，如此方能建構更臻完妥之資通安全防護網。

