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。

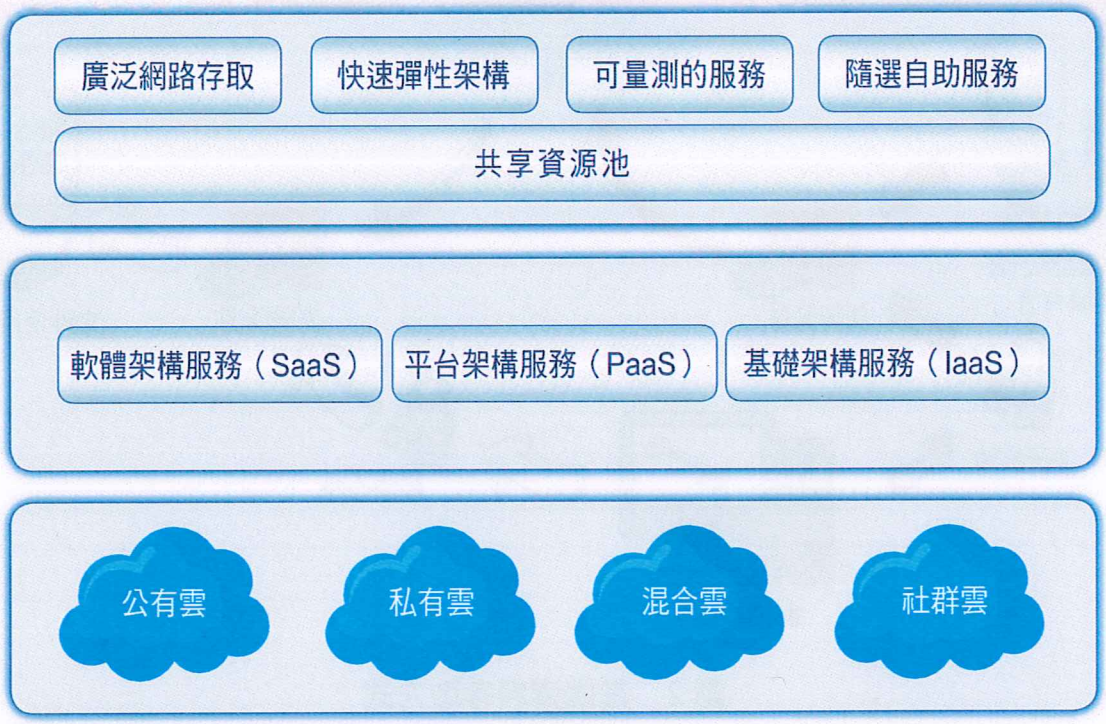

圖 1　雲端架構

（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。

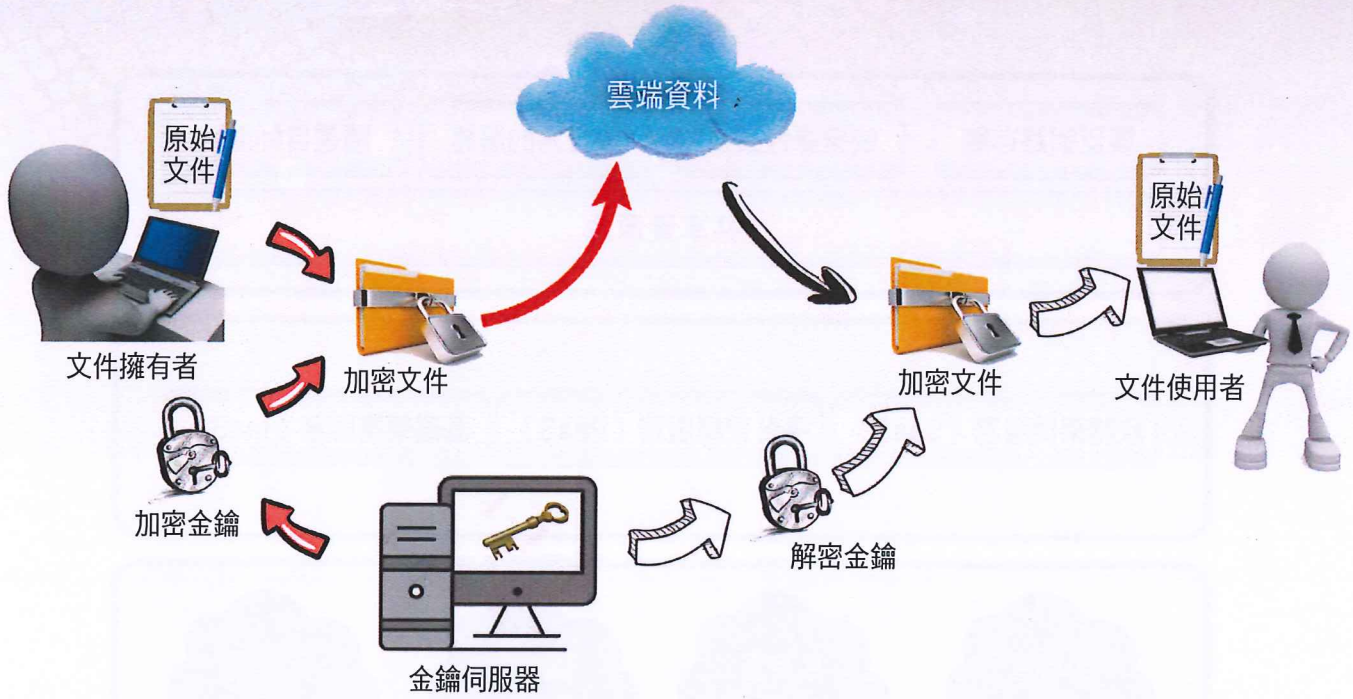

圖 2　雲端資料存取方式

（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。