國立政治大學法學院碩士在職專班

碩士學位論文

# 銀行業與保險業運用雲端服務與個人資料保護之合規研究

# A Study of Compliance with Personal Data Protection about Cloud Service Applied by Banking and Insurance Industry

指導教授：劉定基 博士

研究生：王　綱 撰

中 華 民 國 110 年 10 月

DOI:10.6814/NCCU202101656

# 謝辭

本篇論文的完成首先要感謝指導教授劉定基教授對我的指導。從論文的架構、撰寫到定稿的過程中，劉定基教授給予我許多受用的建議並一一解答我的困惑，讓我可以不斷突破瓶頸，最後達成目標。其次要感謝王立達教授與范姜真媺教授擔任我的口試委員，給予我諸多寶貴意見，使本研究得更為完善。

我也由衷感謝我的家人在論文撰寫期間對我的支持與鼓勵，讓我可以無後顧之憂的全力以赴。並感謝工作上的直屬長官和同事先進給予我重要的提點與資訊，使我論文內容更貼近實務。



DOI:10.6814/NCCU202101656

# 摘要

雲端運算自 2010 年開始商業化迄今已逾 10 年的發展，隨著資訊技術在軟硬體方面的革新、網際網路效能提升和新興行動科技的問世，無論是在雲端服務的模式(如 SaaS、PaaS、IaaS)或是架構(如公有雲、私有雲、混和雲與社群雲)上都逐漸成熟，也使雲端運算在各領域(例如:公部門、醫療、金融、物流等)的運用漸成為趨勢。銀行業與保險業在雲端運算的運用上之前多以私有雲來進行(例如巨量資料分析、區塊鏈的智能合約、智能客服等)，主因是考量法規依據與個資保護等議題，所以對於委外雲端服務大多在評估階段。2019 年 9 月 30 日完成「金融機構作業委託他人處理內部作業制度及程序辦法」修訂後，銀行業與保險業在委外雲端的運用上有較明確的法規依據。日後便可依照相關辦法中所規範的原則建立委外雲端服務的系統架構。

金融機構運用雲端服務的個資保護議題除了與「個人資料保護法」及「個人資料保護法施行細則」有關外，「金融機構作業委託他人處理內部作業制度及程序辦法」、「金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法」、「保險業辦理資訊安全防護自律規範」等都是需要遵守的法規規範。在委外雲端服務的運用上若要符合個資保護的相關規範，就必須在委外雲端服務的合約中訂立適當的條款。合約中對於委外雲端作業的風險控管、委託者的最終監督義務、主管機關和委託者的實地查核權力、查核方式、資料保護機制、受託者權限管理、資料儲存地點及緊急應變計畫等都應在委外雲端服務合約中載明，以利個人資料保護的執行。本篇論文以此想法為出發點，並以目前委外雲端服務中較具規模業者的合約為討論對象，說明一般委外雲端服務合約對於相關法規的涵蓋程度。

關鍵字: 雲端運算、委外雲端服務、個人資料保護、金融業委外雲端服務合約、金融機構作業委託他人處理內部作業

DOI:10.6814/NCCU202101656

# Abstract

Cloud computing has been commercialized in 2010 and developed for more than 10 years until now. With the innovation of information technology about software and hardware, the improvement of Internet performance and the advent of emerging mobile technology, both the model of cloud service (such as SaaS, PaaS, IaaS) and the architecture of cloud service (such as public cloud, private cloud, hybrid cloud and community cloud) are gradually matured. It is a trend that cloud service will gradually be used in various fields (such as public sector, healthcare, finance, logistics, etc.). Banking and insurance industries used private clouds as cloud computing for business purpose (such as big data analysis, blockchain smart contracts, smart customer service, etc.) during the past decade. The major reason is to consider the issues about legal requirement and personal information protection. Therefore, outsourcing cloud service is in the evaluation stage. After completed the regulation revision of the "Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation" on September 30, 2019, banking and insurance industries have more confirmed regulations to obey for the usage of outsourcing cloud service. In the future, a system architecture with outsourcing cloud services can be established in accordance with the principles specified by the relevant regulations.

Besides the Personal Data Protection Act , banking and insurance industry using outsourcing cloud service also need to complied with the “Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation”, the insurance industry also have to abide the insurance industry self-regulatory regulations for information security protection and the security maintenance of personal data files for non-public organization regulations by the Financial



DOI:10.6814/NCCU202101656

Supervisory Commission (FSC). Therefore, the use of outsourcing cloud services must comply with the relevant regulations for personal data protection, it is necessary to establish appropriate terms in the outsourcing cloud service contract. In the contract, the risk control of the outsourcing cloud operation, the final supervision obligation of the client, the on-site inspection powers of the competent authority and the client, the inspection method, the data protection mechanism, the trustee's authority management, the data storage location, and emergency response plans, etc. all should be stated in the outsourcing cloud service contract to facilitate the implementation of personal data protection. This paper uses this idea as the starting point to compare the contracts by the major outsourcing cloud services vendors with the regulation. To analysis the regulation coverage of the general cloud service contract.



Keywords: Cloud Computing, Outsourcing Cloud Service, Cloud Service Contract, Personal Data Protection, SaaS, PaaS, IaaS, Public Cloud, Private Cloud, Hybrid Cloud, Community Cloud

DOI:10.6814/NCCU202101656

DOI:10.6814/NCCU202101656

# 目錄





DOI:10.6814/NCCU202101656

DOI:10.6814/NCCU202101656

DOI:10.6814/NCCU202101656

**附錄**







DOI:10.6814/NCCU202101656

# 第一章　緒論

## 第一節　研究動機與目的

雲端運算(cloud computing)的定義是一種由遠端服務者透過通訊網路提供資訊科技服務(如:軟體、平台、基礎設施)的新興資源利用方式，由於使用者需透過「網際網路」取得服務，而傳統上網際網路的代表符號是一朵「雲」，因此稱為「雲端運算」[1]。雲端運算從資訊科技的發展過程來看大約是在2010年開始有較具體的技術架構，接下來因為網路傳輸寬頻增加、資料分散式的運算和存儲方式、網際網路科技更新及電腦硬體架構虛擬化等新技術的發展而將雲端運算逐漸優化。我國銀行業與保險業對於雲端科技的運用一直持續關注，但是因為雲端科技的複雜度較高，而且金融主管機關(金管會)初期對於雲端科技的運用持保守態度，所以銀行業與保險業並未積極運用。金管會監理方式保守的原因主要是對於雲端科技的資料處理透明度、資訊安全管理及個人資料及隱私權保護的方式都有疑慮，且沒有相關的法規可以直接規範這類型的委外服務。2019年 9 月金管會對於委外雲端服務的運用在「金融機構作業委託他人處理內部作業制度及程序辦法」完成修法後有了明確的規範，這樣的開放使金融相關行業可以較以往擴大運用雲端科技。

修訂後的辦法引起筆者關注的原因是法規修訂前筆者所任職的工作機構不考慮委外雲端的服務，主要理由在於選擇委外雲端服務時沒有較明確的規範可以參考，使公司未來對委外雲端業者的管理，或回應金管會對運用委外雲端服

[1] Renzo Marchini,  Cloud Computing: A Practical Introduction to the Legal Issues, 1.3 What is cloud computing? Page 4, Sep 2010。另參閱劉定基，雲端運算與個人資料保護-以台灣個人資料保護法與歐盟個人資料保護指令的比較為中心，東海大學法學研究第 43 期，頁 55，2014 年 8 月。



DOI:10.6814/NCCU202101656

務的監督稽核時，恐有缺失無法完全改善的風險。辦法修訂後雖然有了較明確的規範可以遵循，但是對於金融機構實際運用委外雲端服務時該如何配合相關監理規定，仍有不少值得注意或有待釐清的地方。因此筆者以在保險公司資訊部工作者的角度觀察，並且透過委外雲端服務合約實例的分析，希望能瞭解市面上委外雲端服務合約與新法規的配合程度，藉此提供金融機構評估委外雲端服務合約時的參考[2]。

## 第二節　研究範圍與方法

本論文的研究範圍以銀行業與保險業的委外雲端服務為限。行業別範圍的選擇是以筆者個人所處行業的實務經驗再加上銀行業與保險業在雲端服務的運用有別於其他行業，所以定此範圍。雲端服務以「委外」雲端服務為範圍，是以企業的角度將資訊相關業務委託雲端服務業者為討論的對象，將個人雲端郵件服務、個人雲端存儲服務等屬於個人類的雲端服務排除討論範圍。

本研究所採取的研究方法為「文獻分析法」。筆者蒐集銀行業與保險業在運用雲端服務的相關資料以說明實務現況，進一步分析未來可能的發展與委外雲端服務的運用，同時分析及歸納有關雲端服務在資訊安全、個人資料保護和隱私權保障等方面的相關文獻，並對於委外雲端服務相關法規文獻提出目的說明和分析可行性。以委外雲端服務合約的實例文件來分析是否達到合規的要求及提出建議。

[2] 李治安，雲端運算相關法律問題初探，財經法新課題與新趨勢，頁 555-556，2011 年 5 月。請參閱「二、契約民事責任問題」對於和雲端服務廠商簽訂合約時因雙方議價能力不相當的形況下須考慮的問題 。



DOI:10.6814/NCCU202101656

## 第三節　研究架構

本論文分成五章，以下大略介紹各章的討論重點:

第一章為緒論，說明研究動機與目的、研究範圍與方法以及研究架構。

第二章是對於雲端科技的發展過程與內容作說明。包含雲端服務的類型[3]：基礎設施即服務(Infrastructure as a Service, IaaS)、平台即服務(Platform as a Service, PaaS)和軟體即服務(Software as a Service, SaaS)。雲端服務的架構[4]可以區分為公有雲(public cloud)、私有雲(private cloud)、混和雲(hybrid cloud)及社群雲(community cloud)等。本章對於雲端服務的優點和挑戰也會說明。由於本論文所聚焦的產業是銀行業與保險業，所以會針對該二行業運用雲端運算的情形特別加以說明。以目前發展及應用來看，區塊鏈、巨量資料分析以及 IT 維運這三方面有較具體的成果。因此會對於銀行業及保險業在區塊鏈與雲端運算的結合應用說明。此外，雲端運算在巨量資料的分析應用上，銀行業與保險業也有相當的投入。最後，是IT部門在維運上運用雲端運算可以達到的成果。

第三章討論銀行業與保險業在運用雲端服務時資訊安全及個資保護會所面臨的議題。委外雲端服務在服務架構上會有一般性的資訊安全議題，但是當銀行業與保險業在運用雲端服務時也會有特殊性的資訊安全議題需要討論。個資保護議題雖然與資訊安全有關，但是和資訊安全的關注重點仍有差異[5]。最後關

[3] John W. Rittinghouse, James F. Ransome, Cloud Computing Implementation, Management and Security, CRC Press, 2010. 2.3, 2.5, 2.6.

[4] 廖文華、張志勇、蒯思齊，雲端運算概論，五南圖書出版股份有限公司，頁 13，2021 年 2 月。

[5] 范姜真媺，個人資料保護法關於「個人資料」保護範圍之檢討，東海大學法學研究第 41 期，頁 91-123，2013 年 12 月。



DOI:10.6814/NCCU202101656

於保險業因為所蒐集處理利用資料的特殊性，會從保險業業務流程的角度來說明運用委外雲端服務的個人資料保護議題。

第四章分析討論我國銀行業及保險業在運用委外雲端服務時所必須遵循的規範與個人資料保護的議題。法規部分包含「個人資料保護法」、「個人資料保護法施行細則」、「金融機構作業委託他人處理內部作業制度及程序辦法」、「保險業作業委託他人處理應注意事項」、「保險業辦理資訊安全防護自律規範」[6]和「金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法」。其中「金融機構作業委託他人處理內部作業制度及程序辦法」於 2019 年完成修正後成為銀行業與保險業運用委外雲端服務時直接的規範依據，而其他規範也直接或間接與委外雲端服務相關，共同構成金管會對於使用委外雲端服務的監理框架。本章在說明法規後接著說明委外端雲服務合約應注意的事項，之後並以委外雲端服務實際合約為範例說明合約相關內容，進一步再用個資保護相關法規檢視合約合規的程度。

第五章為結論，將總結歸納本論文的研究結果。

[6] 趙偉傑，規範制定公私協力之研究—保險業內部控制及稽核監理法治為例，國立政治大學法律學系研究所碩士學位論文，頁 136-137，2019 年 5 月。請參照「第三款商業同業公會自律規範」相關說明。



DOI:10.6814/NCCU202101656

# 第二章　雲端服務之發展與我國銀行業與保險業之運用

本章將說明雲端服務的發展過程與雲端服務的內容。雲端服務的發展是隨這電腦科技的進步而逐漸演進而來的，是一連串技術和觀念互相影響的結果。雲端服務的內容包含的類型和架構，雲端服務的類型有基礎設施即服務(Infrastructure as a Service, IaaS)、平台即服務(Platform as a Service, PaaS)和軟體即服務(Software as a Service, SaaS)。雲端服務的架構有公有雲(Public Cloud)、私有雲(Private Cloud)、混合雲(Hybrid Cloud)和社群雲(Community Cloud)。雲端服務和其他資訊科技一樣都會有優點及面對的挑戰。我國銀行業與保險業在雲端服務的運用上有持續的投入，目前可見到具體成果包括使用雲端服務的區塊鏈、巨量資料分析及企業資訊部門的維運。本章也會對於這三方面說明現階段的發展狀況。

## 第一節　雲端服務之形成及內容

### 第一項　雲端服務之形成

雲端科技可以視為是電腦科技的革新。所謂革新，不是單指技術，包含概念。從 1974 年電晶體問世開始，電腦的發展開始有了加速的成果[7]。1950 年代至 1960 年代之間，電腦的發展雖然快速，但是大都是以大型主機為硬體架構的發展框架，不管是在內部的組合元件或是外部的輸出與輸入的媒介上，此時的電腦只能運用在特定的機構如政府或學術單位為特定的目的服務，對於一般機

[7] 廖文華、張志勇、蒯思齊，前揭註 4，頁 5-6，「1-2 雲端運算的演進和技術」中對於電腦科技的發展歷史從 1947 開始說明至 1981。



DOI:10.6814/NCCU202101656

構及個人在使用上並未普及。Intel 在 1969 年開發出第一顆微處理器之後，1970 年代成為個人電腦(PC)開始發展的時代，接著 IBM 於 1980 代開始積極投入個人電腦的開發與銷售，所帶來的進步是硬體執行效率的提升與使用者介面優化，同時也朝縮小化進步，日後筆記型電腦、平板電腦及手持型行動設備的基礎。同時期大型主機的地位並未因此動搖，反而成為大容量高效率的表徵，電腦科技開始朝向企業化設備及個人化設備的雙引擎發展，將電腦科技的革新速度與功能不斷翻轉[8]。

在此同時，另一項不可忽略的發展則是網路。最早的網路發展可以追朔至 1969 年的 ARPANET[9]。在當時在這樣的連接技術下使電腦之間可以開始互相溝通，至 1981 年為止約有近 200 個組織的電腦可以在這個網路上相互聯結。Internet 起初也只限於國防及科學上的研究，但自 1988 年開始 Internet 的使用範圍擴大至商業領域，不過也只是在 email、Telnet 及 Usenet 等。直到 1989 年網際網路(World Wide Web, WWW[10])的問世才使 Internet 有了突破性的發展。WWW

[8] 同前註，頁 6。

[9] 國家教育研究院，雙語詞彙、學術名詞既辭書資訊網，「在 1960 年代末期開始，由美國國防部的先進研究計畫機構所從事計算機網路研究的成果，這個網路連接了猶他大學、UCLA、UCSB 和史丹福研究協會，以作為　和美國國防部的研究通道，是計算機網路研究的先驅。其所使用的通訊協定為 TCP/IP 協定組，其發展早於開放式系統互連參考模型（OSI），所以並未遵循 OSI 的架構，造成 TCP/IP 協定在今日成為最重要的通訊協定之一，並發展成為全球性的網際網路。參【高級研究規劃局；高級研究規劃局網路】（ARPA）

[10] 同前註，「全球資訊網（World Wide Web），簡稱 Web、WWW 或 W3，是一套建構於網際網路（Internet）之上，藉由超連結（hyperlink）將分散於全球各地的圖、文、影、音等多媒體資料加以整合應用的資訊系統。雖然在 Web 出現之前，網際網路上已有 e-mail、FTP、newsgroup、Gopher、BBS 等應用或服務，但直到 Web 之後，才真正實現超媒體（hypermedia）整合的理想。1980 年代至 1990 年代期間被視為是當今全球資訊網的萌芽期。1980 年時，任職於歐洲核子研究組織（European Organization for Nuclear Research，簡稱 CERN）的 Tim Berners-Lee，實作了一套稱為 Enquire 的小型超文件軟體系統，供 CERN 研究人員用來分享文件資料。然而，CERN 是一個龐大的研究組織，擁有數以千計的研究人員且分散於不同部門，日積月累所產出的文件資料量相當多，因此要如何更有效記錄、管理、分享與查找，才不致於遺漏重要資訊，便成了一個重要課題。Tim Berners-Lee 遂於 1989 年 3 月提出了一份名為"Information Management: A Proposal"的計畫構想書，認為採用 1960 年代由 Ted Nelson 所提出的超文件（hypertext）概念，進而開發出通用的連結資訊系統（universal linked information system），使得所有資訊皆能互相連結並有效存取，才是最有效的解決方案。因此，基於先前實作 Enquire 的經驗，Tim Berners-Lee 及其同事經過一年多的努力，終於在 1990 年底完成了建構全球資訊網的基礎工作：制訂超文件傳輸協定（HyperText Transfer



DOI:10.6814/NCCU202101656

最開始是為了歐洲核能研究組織(CERN)的資訊管理系統，採用文件超連結(Hypertext)的技術。這個技術的觀念就是經由一個邏輯的參考點來取得相關的知識內容。而當時 Mosaic 瀏覽器的推出，也是將 WWW 推為風潮的主因。接著網路技術在頻寬不斷增加及網路設備效能倍增的助力之下，輔以相關程式語言的開發，如 Java、PHP 等，使得在 Internet 上開始有互動式的網站應用，除了一般人所熟悉的多媒體網站或購物、社交等平台之外，開始有應用程式部署的做法出現，像是辦公室所使用的文書處理及試算表程式等。此時在硬體建置上也有新的觀念出現，像是網格計算(Grid Computing)。雲端運算的名詞則出現在 2007 年，主要是將硬體和軟體一起部署，當時是由 Google、IBM 和數間美國大學一起研究[11]。這個雲端運算計畫原意是要降低分散式運算技術在學術研究上的成本，讓學生可以利用網路進行需要大規模運算資源的研究計畫。日後這個計畫被視為雲端運算的初始計畫。從 2008 年起陸續有資訊科技公司如惠普、戴爾、Intel、AMD 等投入雲端運算的研究開發，至 2010 年雲端運算開始有具體的模式推出。

雲端運算模式的是從集中式運算(Centralized Computing)、叢集式運算(Cluster Computing)、分散式運算(Distributed Computing)一路演進至網格計算(Grid Computing)而來的。分別說明如下:

一、集中式運算模式

---

Protocol，簡稱 HTTP）和超文件標示語言（HyperText Markup Language，簡稱 HTML），開發全世界第一套 Web 瀏覽器暨編輯器軟體和第一套 HTTP 伺服器軟體，建置全球第一個網站和撰寫第一個網頁。1991 年 8 月 6 日，Tim Berners-Lee 在網路新聞群組上簡要說明了全球資訊網計畫，這一天便被認定是 Web 首次對外公開的日子。」

[11] 廖文華、張志勇、蒯思齊，前揭註 4，頁 6，「1-2 雲端運算的演進和技術」中對於 Internet 發展的過程與促成資訊技術的改變。



DOI:10.6814/NCCU202101656

電腦初期的運算模式是以集中式的模式為基礎。集中式的運算模式強調高運算能力的硬體設備，所以此時的主流是大型主機(如 IBM Mainframe)和超級電腦(如 IBM 7030)，主要用於大量資料運算或是特殊專案的資料處理，像是銀行金融交易、政府戶口普查及特殊國防專案需求等。此一運算模式的重心在於大規模的資料輸出與輸入。有些大型電腦可以同時執行多作業系統，因此與其說是一台電腦，不如說是多台虛擬機器。像是一台主機但是提供多台伺服器的概念，這算是虛擬化架構的先驅。超級電腦可以執行一般個人電腦所無法處理的大量資料與高速運算，其基本元件與個人電腦概念相同，只是在規格上強大許多。伴隨處理器的發展從 1960 年代的單一處理器到 1970 年代的多工處理器，1980 年代資訊科技業開始大規模發展平行運算系統，超級電腦可以視為由多數普通處理器所組成的運算機器[12]。

二、叢集式運算模式

叢集式運算模式的產生是為普及資訊科技之應用所自然形成的趨勢。畢竟大型主機與超級電腦無論是在硬體設備及空間建置的需求上都不是一般企業或機構可以負擔的。當電腦處理器的功能及效能均日益增強之後，開始設計出同一地點內可將各自獨立的硬體與軟體透過區域網路(LAN)進行結合，以協同合作方式完成運算工作，這樣的設計是將數台電腦整合成一台電腦執行相同的工作。如此同時解決需要較強運算能力但卻無法負擔大型主機與超級電腦的痛點[13]。

[12] 同前註，頁 7，請參考「集中式計算」的說明。另參考 Angelo F. Corridori, What is Centralized Computing, http://zseries.marist.edu/enterprisesystemseducation/zinsights/ECI%20No.%202%20Cent%20Comp%20v2c.pdf.

[13] 同前註，頁 7，請參考「叢集式計算」說明。另參考 WatElectronic, Cluster Computing:



DOI:10.6814/NCCU202101656

三、分散式運算模式

分散式運算是運用區域網路或廣域網路(WAN)將個別獨立的軟硬體結合以便達到資源整合的目的。在此運算架構之下，是把需要運算的大量資料分割成若干區塊，而由多台電腦進行個別運算，再將個別運算結果上傳總和最終結果。會有這樣的發展應該有兩個因素促成，第一是網路傳輸技術的進步。網路傳輸的技術與能力不斷提升，使電腦運算不必拘泥於實體位置，可以依照需要將運算節點分散只需在最後做整合即可。這一點對於一些跨業界結合的商業行為十分有利，因為它可以整合不同組織內的運算資源，而產生對使用多方都有利益的結果，有作業分工與資源共享的概念。第二是災害備援的需要。分散式運算因為是將各運算單位分散在異地，所以對組織來說是非常重要的資安考量。分散式運算在當有災害備援的需求時，可以有較彈性的調度與使用[14]。

四、網格運算模式

網格運算模式是分散式運算模式的進階化。因為電腦的不同作業系統間已經可以整合，所以網格運算的原理是透過整合大量桌上型電腦的未用資源如 CPU 和磁碟存處等，將這些資源建立成一個在電信網路上的虛擬電腦集群。由於此一虛擬電腦集群是將不同類類型的軟硬體資源透過網路進行高度整合，可以視為將原本以同質性整合為主的分散式運算模式又往前推進一步[15]。

---

Architecture & Its Types, https://www.watelectronics.com/cluster-computing-architecture-its-types/.

[14] 同前註，頁 7，請參考「分散式計算」說明。另參考 IONOS, Distributed computing for efficient digital infrastructures, https://www.ionos.com/digitalguide/server/know-how/what-is-distributed-computing/.

[15] 同前註，頁 7，請參考「網格計算」說明。另參考 Jonathan Strickland, How Grid Computing Works, https://computer.howstuffworks.com/grid-computing.htm.



DOI:10.6814/NCCU202101656

五、雲端運算模式

雲端運算模式是經過上述各階段運算模式發展後的結果。雲端運算已經不再只是以資訊科技為導向的發展，而是以網際網路為基礎的服務模式，提供具有動態及彈性的使用者需求滿足，並且以資源虛擬化的技術來達到前述的目標。使用者可以透過瀏覽器、桌面應用程式或是行動應用程式來使用雲端服務[16]。企業也因此可以迅速部署應用程式，而且降低管理複雜度與維護成本。綜合言之，雲端運算模式包含以下的元素而成為以服務為導向的架構(SOA)：虛擬化及多核心處理器的硬體規格、Web 服務為基準的網際網路架構、資料中心自動化的系統管理與分散式計算的運算原理[17]。

回顧雲端運算的產生也並非一夕之間所促成，資訊科技不斷進步，再加上資訊科技的應用概念不斷變革，在互相帶動之下，雲端運算從發想醞釀、試驗性推出、到近來商業化廣泛運用，在愈發成熟的架構下，雲端運算已經成為現代人生活中的一部份。

## 第二項　雲端服務的模式

雲端服務的模式可以分成三種: 基礎設施即服務(Infrastructure as a Service, IaaS)、平台即服務(Platform as a Service, PaaS)和軟體即服務(Software as a Service, SaaS)。

---

[16] 同前註，頁 7，請參考「雲端運算」說明。另參考 Steve Ranger, What is cloud computing? Everything you need to know about the cloud explained, ZDNet, https://www.zdnet.com/article/what-is-cloud-computing-everything-you-need-to-know-about-the-cloud/.

[17] 同前註，頁 8-10，請參考雲端運算說明中關於重要的技術，「網格計算與功用計算」、「自主計算(Autonomic Computing)」、「Web 服務、服務架構導向(Service Oriented Architecture, SOA)」、「虛擬化技術」。



DOI:10.6814/NCCU202101656

在基礎設施即服務中(IaaS)，主要是提供雲端運算裡基礎架構的服務，包含資料運算、資料存儲、網路通訊等資源，以虛擬化的方式建構。虛擬化機器資源透過監控器加以管理，資源池的管理可以依據使用者的需求動態調整虛擬機的數量與運作。此外還提供如虛擬機映像(VMI)、防火牆、IP位置、虛擬區域網路(VLAN)、網路流量平衡負載(load balance)及基礎架構層的軟體套件等。使用者可以依照需求，透過網際網路在雲端服務中心彈性化的使用這些資源。主要的使用對象為資訊部門中基礎設施的維運及管理人員[18]。

平台即服務(PaaS)主要提供開發的平台。包含作業系統、程式語言的執行環境、資料庫、網頁伺服器等。此類型的使用者主要為應用程式開發人員。應用程式開發人員可以透過這樣類型的雲端服務在平台上開發和執行所需的應用程式，無須考慮到購買和維護軟硬體的複雜度與成本。此外在此類平台上執行應用程式時，也無須手動調整相關資源，此類型平台在執行應用程式時會依照執行時的需求自動調整資源至最適宜狀態。使用者使用主機操作應用程式並掌控運作應用程式的環境（也擁有主機部分掌控權），但並不掌控作業系統、硬體或運作的網路基礎架構[19]。

軟體即服務(SaaS)不同於傳統應用程式，它具備高度彈性。在此類型的服務平台中，應用程式是建置於雲端環境並且在雲端中執行，雲端使用者透過終端使用軟體直接使用，無需管理基礎設施與平台。在這樣的雲端服務類型下，應用程式在執行時可以複製多份到虛擬機器上同時執行，滿足執行效率同時也可以兼顧資源使用上的平衡。此類服務的使用者多半屬於應用程式的使用人員。人員使用應用程式，但並不掌控作業系統、硬體或運作的網路基礎架構。是一

[18] 同前註，頁 11，請參照「1. 基礎設施即服務 (IaaS)」相關說明。

[19] 同前註，頁 12，請參照「2. 平台即服務 (PaaS)」相關說明。



DOI:10.6814/NCCU202101656

種以服務為基礎的觀念，軟體服務供應商，以租賃的概念提供客戶服務，而非購買，比較常見的模式是提供一組帳號密碼[20]。

這三層的服務類型其實是互有關連性的。較高層的服務是由較低層服務來建構。雲端基礎設施服務層中的核心中介軟體主要管理實體資源，而虛擬機就部署在這層。此層同時支援多用戶使用模式。而開發環境層則建立在基礎設施服務層之上，提供應用程式開發和部署的能力。此層中還提供各種程式模組、程式庫、API 等開發相關原件。以上兩層都算是軟體服務的支援架構層，這樣便可以對於只需軟體服務的使用者提供更為完整且彈性的雲端服務[21]。

### 第三項　雲端服務的架構

雲端服務的架構應該從雲端部署的角度來看。當企業在考慮雲端服務的使用時，會有基本的因素要納入評估，像是系統整合成本、營運成本、系統可靠度、資訊安全等。基於不同因素的比重考量，會有不同的部署架構。雲端部署可以分為四種架構: 公有雲(Public Cloud)、私有雲(Private Cloud)、混合雲(Hybrid Cloud)和社群雲(Community Cloud)。

公有雲是雲端服務廠商將運算及儲存資源開放給一般大眾使用，像 Amazon 的 AWS、Google 的 GCP 和 Microsoft 的 Azure 都是這種服務架構。公有雲服務商提供運算、存儲和應用程式資源給使用者，企業或用戶透過網際網路來使用這些服務，並且以隨用隨付的方式計價。這種模式的好處是使用者可以不必自己投入大量資源做資訊技術的環境建置，節省資源並保有迅速和彈性。但在使用者對於雲端服務屬於低度控管的情況下，對於資料控制、網路和資安的機制

[20] 同前註，頁 12，請參照「3. 軟體即服務 (SaaS)」相關說明。

[21] 同前註，頁 11，請參照「1-3 雲端運算的架構」相關說明。



DOI:10.6814/NCCU202101656

是有疑慮的[22]。

私有雲也稱為內部雲。私有雲的建立通常是企業或組織為了私用所設計的。私有雲在效率、可靠度即安全上有高度控制力。私有雲具備許多公用雲環境的優點，例如彈性、適合提供服務，兩者差別在於私有雲服務中，資料與程式皆在組織內管理，且與公用雲服務不同，不會受到網路頻寬、安全疑慮、法規限制影響；此外，私有雲服務讓供應者及使用者更能掌控雲端基礎架構、改善安全與彈性，因為使用者與網路都受到特殊限制[23]。

混和雲顧名思義是結合公有雲和私有雲的架構，是一種期望將前述兩種架構的優點同時保有的複合式架構。在混合雲中，有一部分的服務是在公有雲中執行，其他部分則是在私有雲中執行。混合雲比起公有雲和私有雲更具有彈性，企業使用混合雲可以彌補公有雲在資料控管以及資安維護上的低度控管，也可以將私有雲需要自己建置與管理的負擔部份轉嫁於公有雲而降低。但是在設計混合雲時非常需要注意的是公有雲和私有雲結合的分割點。尤其是企業對公有雲與私有雲的分工模式以及公有雲和私有雲的傳輸界接方式與控管，會是混合雲要考量的重點[24]。

社群雲主要是一些組織有共同特定的目的所建立的共享式雲端服務架構。社群成員共同使用雲端資料、應用程式、共享的雲端基礎設施。社群成員支持特定的社群及有共同的關切事項，例如使命任務、安全需求、策略與法規遵循考量等。管理者可能是組織本身，也能是第三方；管理位置可能在組織內部，

[22] 同前註，頁 13，請參照「公有雲 (Public Cloud)」相關說明。

[23] 同前註，頁 13，請參照「私有雲 (Private Cloud)」相關說明。

[24] 同前註，頁 13，請參照「混和雲 (Hybrid Cloud)」相關說明。



DOI:10.6814/NCCU202101656

也可能在組織外部[25]。

### 第四項　雲端服務的優點與挑戰

究竟雲端服務有何優點，我們可以從美國國家科技標準機構 (NIST, National Institute of Standards and Technology)所描述的五個雲端運算的特徵加以說明[26]:

一、隨選所需 (On-demand self-service):

使用者可以依照所需要的服務選擇適合的雲端運算資源，例如伺服器運算能力或是需要儲存的資料量等[27]。

二、廣泛網路存取 (Broad network access):

雲端服務是透過標準化使用介面提供多種介面存取，例如智慧手機、筆記型電腦及平板電腦等[28]。

三、資源共享 (Resource pooling):

雲端運算的架構是將各種虛擬或實體的資源加以集中，而使用者以共享的方式使用資源。這是一種「資源池」的概念。使用者不需了解資源所在位置的細節，而雲端服務在資源調度上會依照使用者的需要進行提供，因為提供方式

---

[25] 同前註，頁 13，請參照「社群雲 (Community Cloud)」相關說明。

[26] 黃正傑，雲端運算運用與實務，全華圖書股份有限公司，頁 2-13，2018 年 9 月。NIST 對雲端運算的定義為「雲端運算是一種無所不在、便利、隨選所需(on-demand)的網路資源存取模式。使用者可以存取可配置的共享電腦運算資源池 (如: 網路、伺服器、儲存設備、應用程式與服務)，並在最少的管理成本或服務供應商的互動下，快速地完成服務佈署與發佈」。

[27] 同前註，頁 2-15，請參照「1. 隨選所需 (On-demand self-service)」。

[28] 同前註，頁 2-15，請參照「2. 廣泛網路存取 (Broad network access)」。



DOI:10.6814/NCCU202101656

是以網際網路為基礎[29]。

四、迅速及彈性的調整服務 (Rapid elasticity):

雲端運算的資源可以視需要而彈性調整，依照尖峰時期與離峰時期的資源運用差別而予以適切的資源配置，脫離傳統 IT 資源規劃的限制[30]。

五、可衡量與計價的服務 (Measured service):

雲端運算資源的彈性使用，反映在計價的模式上自然可以視所使用資源的多寡進行量化後依照使用付費的概念進行收費，合理反映資訊系統因使用資源類型和數量不同而有成本負擔不同的結果[31]。

雲端服務雖然有其優點，但是企業要導入雲端運算也面臨以下的挑戰:

一、安全性與隱私性

雲端服務的架構與技術組合是一項全新的模式，在這樣的組合之下，安全性的評估一直也是是否採用雲端服務的主要考量。雲端運算是網路層、主機層、應用層和資料層的互聯協同運作，這種新的整合方式在安全上的可信任度其實是很模糊的。與安全性有相關的是隱私性的議題。雲端運算既然是一種新的服務模式，其服務是否符合隱私法規的規範也一直備受挑戰。企業在使用雲端運算的同時，需要考慮對個人資料保護的強度是否足夠，並可以提出相關的證明來驗證雲端服務對隱私保障的適足性，相關的監督成本也會成為企業是否採用

[29] 同前註，頁 2-15，請參照「3. 資源集中 (Resource pooling)」。

[30] 同前註，頁 2-15，請參照「4. 快速、彈性地調整服務 (Rapid elasticity)」。

[31] 同前註，頁 2-15，請參照「5. 可衡量與計價的服務 (Measured service)」。



DOI:10.6814/NCCU202101656

雲端服務的重要考量之一[32]。

二、可靠性

當企業使用雲端服務時，其實是一種委外服務。現今企業在應用系統上的運行，以 24 小時不間斷的標準愈來愈普遍。因此當考慮使用雲端服務時，將系統中斷時的備援機制納入考量是十分普遍的著眼點。雲端服務業者可否有能力提供無縫接軌的備援機制會是企業是否要採用雲端服務的考量因素[33]。

三、互通性與獨立性

互通性是指企業在考量自建系統與雲端系統整合性的問題。而獨立性則是指雲端服務業者間服務可否順利移轉的考量。在雲端服務商業化之前，大部分的企業都是在企業內部的 IT 環境中維運。當企業開始評估雲端服務的時候，首先遇到的議題就是要把那些系統服務雲端化。這個議題會有兩種處理方式，第一是將新的系統需求雲端化，另一種則是將既存系統中可以雲端化的部分轉化成雲端服務。無論是哪一種方式，都必須面對在雲端的外部系統與在企業內部環境系統的互通性問題。企業內部的既存系統通常有其發展背景，在以系統穩定度為前提之下，所使用的技術往往與主流科技有至少二至三代的差距。在雲端服務標榜當前主流科技的同時，建置在雲端的系統與建置於企業內部系統的互通性高低會影響企業在使用雲端服務的意願。這種因為使用雲端服務所需要做的系統升級成本往往是關鍵因素[34]。

---

[32] Tim Mather, Subra Kumaraswamy, Shahed Latif，胡為君 譯，雲端資安與隱私企業風險對應之道，頁 31，2012 年 5 月。請參照「安全性」和「隱私性」說明。

[33] 同前註，頁 31，請參照「穩定性」說明。

[34] 同前註，頁 31，請參照「互通性」和「CSP 獨立性」說明。



DOI:10.6814/NCCU202101656

另外，目前市場上的雲端服務業者多半仍有其各自的獨立性，包含各家自有的技術管理模式與維運服務流程等。這樣的情況對於企業來說，一旦選定一家雲端服務業者之後，想要再切換至其他的雲端服務業者是相當困難的一件事。這樣的因素會讓企業考量雲端服務的彈性時有所猶豫。

四、經濟價值

雲端服務的優勢是資源佈署彈性且迅速，利用共享的概念可以讓使用者僅須對自己所使用的部分進行費用的分攤。這對於企業在短期或是臨時性、專案性的系統建置的確有其經濟價值。但值得進一步考慮的是長期的系統維運。企業中的核心系統，從時間軸的角度來看，多半是呈現長期穩定的成長，無論是使用資源或是程式架構的擴張都是如此，企業如果對這類的系統進行長期投資，其資產分攤和折舊的過程對企業的財務並不是一種負擔，但是如果將這類系統以雲端服務的方式來進行，那就是持續的費用支出。隨著系統日漸龐大，雲端服務費用支出就會逐漸上升，長期下來未必會有經濟上的利益[35]。

五、IT 治理與 IT 組織的改變

雲端服務的使用對企業的 IT 部門衝擊是相當大的。無論是從 IT 部門的治理面或是組織面都會產生質的改變。當企業評估雲端服務時，最先要做的是 IT 資產的盤點與資源的整併。IT 以往的運作多半是為配合企業各部門的需求不斷修改或新增系統與程式。無形之中會造成 IT 資源的膨脹與重複購置。如果企業要接軌雲端服務，絕對不是單純的將現在所有的系統使用資源全部移植到雲端服務就好，因為這樣只會造成 IT 費用的暴增。IT 部門首先須對系統的資產進行盤

[35] 同前註，頁 32，請參照「經濟價值」說明。



DOI:10.6814/NCCU202101656

點，包含軟硬體、系統數量與程式碼、管理工具及備份方式等，然後將過多的或重複的資源加以整併，達到 IT 資源輕量化的目標。接下來是依各系統對業務的影響性進行優先順序的排序，最後評估出可以並需要使用雲端服務的目標系統進行雲端服務的整合[36]。IT 人員同時需要了解和學習雲端服務導入後的 IT 維運模式及相關管理工具與流程。IT 的治理不再是單純以系統維運出發，管理軟硬體及網路即可，而是成為企業商業目標達成的推手，根據業務部門的需求從雲端服務中選擇適當的解決方案，快速導入而不需花費過多時間與人力建置。IT 人員成為資訊技術的管理者，這是工作內容與角色的轉型。另外以往 IT 的組織會依照基礎建設(包含伺服器、網路設備、電信設備、機房維運等)、程式開發、資訊安全等功能規劃，在導入雲端服務之後，IT 的人員將脫離以技術為主的功能，比較走向 IT 顧問的功能，所以維運人員需求將會減少，顧問型與管理型的人員將會增加，會造成 IT 的組織變動[37]。

六、跨國界雲端服務所帶來的政治議題

雲端服務的另一個考量是資料所在的國界議題[38]。在雲端服務中，無論是資料所存放的實體位置、資料處理的所在地點、存取資料的所在地等，都有可能是跨國境的司法管轄問題[39]。企業在使用雲端服務時，需要根據雲端服務業者提供服務的架構，去考量可能的跨國界管理問題，以及雲端服務業者註冊所在國的管轄問題，當前述國家的機關介入而要求提供資料及配合調查時，企業必須考量對所屬資料的保護風險及企業所在國的監管要求[40]。目前以國際間對

[36] 同前註，頁 32，請參照「IT 組織中的改變」說明。

[37] 同前註，頁 256、265，請參照「雲端運算對於企業 IT 角色的影響」說明。

[38] 同前註，頁 33，請參照「世界村帶來的政治問題」說明。

[39] 同前註，頁 14-17，請參閱「14-3-2 法律規範」。

[40] 許銘瑋，雲端服務之個人資料保護問題，刑事法雜誌第 62 卷第 2 期，頁 97-99，2018 年 4



DOI:10.6814/NCCU202101656

於洗錢、反資恐及個資保護(如 GDPR)等的態度，對雲端服務的控管力道只會逐漸增強。這是企業要進入雲端服務前必須要慎思的課題，也會是挑戰。

## 第二節　我國銀行業與保險業運用雲端服務和區塊鏈

### 第一項　區塊鏈說明

區塊鏈(Blockchain)的概念是數位事件的紀錄或是分類帳簿，可以在許多不同個體之間分發或是共享事件。該帳本必須取得在大部分鏈系上參與者的認肯才進行紀錄的更新。資訊一旦輸入且被承認，將永久保存。所以區塊鏈的特色之一就是記載著從開始之後的每一筆確定且可以被驗證的交易紀錄。區塊鏈的架構是採分散式帳本技術(Distributed Ledger Technology, DLT)，是運用先進的加密技術來創造具安全性的資訊分類帳本，可以防止未經授權的數字修改、增加或是刪除。在此優勢下，強固的資訊安全和清晰完整的稽核軌跡成為區塊鏈的優勢之一，也因此區塊鏈是不需要中央單位的監督。透過運用分散式帳本還可以增強與第三方機構間的信任並進行資訊交換進而商業交易[41]。綜合觀之，區塊鏈的特性可以歸納如下:

一、分散式的 (Distributed): 所有區塊鏈的參與者都有完整一致的分類帳簿副本，可以達到完全透明的原則。[42]

二、匿名的 (Anonymous): 區塊鏈的參與者可以使用假名為其身分，甚至也可以

---

月。請參照「貳、個資法效力範圍」。

[41] 李顯正，保險科技，新陸書局股份有限公司，頁 397，2020 年 1 月。請參照「9.1.2 區塊鏈的運作模式」章節中「一、什麼是區塊鏈」。

[42] 同前註，頁 401，請參照「9.1.3 區塊鏈的類型與特性」章節中「二、區塊鏈的特性」有關分散式的說明。



DOI:10.6814/NCCU202101656

匿名使用，因此具有高度保密性。[43]

三、具時間紀錄 (Time stamped): 區塊鏈中，每筆交易都會有時間戳記紀錄於一個區塊中，交易紀錄的時間順序清晰。[44]

四、共同肯認的 (Consensus): 區塊鏈中所有紀錄都必須得到參與者的認肯才會有效。[45]

五、可編輯程式的 (Programmable): 區塊鏈的程式是可以編輯和客製化的，可以依照需求而編輯所需的程式。[46]

六、安全性 (Secured): 區塊鏈中所有紀錄均經過單獨加密。[47]

七、不可更改的 (Immutable): 區塊鏈中任何經過驗證的紀錄都是不可逆也無法更動的。[48]

因為區塊鏈的上述特性，因此銀行業與保險業開始思考及研究區塊鏈技術在組織內部及產業的可行性應用，甚至認為此一運用將會改變服務的價值鏈，

---

[43] 同前註，頁 401，請參照「9.1.3 區塊鏈的類型與特性」章節中「二、區塊鏈的特性」有關匿名的說明。

[44] 同前註，頁 401，請參照「9.1.3 區塊鏈的類型與特性」章節中「二、區塊鏈的特性」有關帶時間戳記的說明。

[45] 同前註，頁 401，請參照「9.1.3 區塊鏈的類型與特性」章節中「二、區塊鏈的特性」有關共識的說明。

[46] 同前註，頁 401，請參照「9.1.3 區塊鏈的類型與特性」章節中「二、區塊鏈的特性」有關可編程的說明。

[47] 同前註，頁 401，請參照「9.1.3 區塊鏈的類型與特性」章節中「二、區塊鏈的特性」有關安全的說明。

[48] 同前註，頁 402，請參照「9.1.3 區塊鏈的類型與特性」章節中「二、區塊鏈的特性」有關不可更改的說明。



DOI:10.6814/NCCU202101656

創造一個更安全、更有效率的商業流程。

隨著技術和需求的發展，區塊鏈的型態目前主要有三種:

一、公共區塊鏈 (Public Blockchain): 此一類型的區塊鏈，所有參與者都可以進行資料庫查詢、副本儲存，並透過提供運算能力進行資料的修改。[49]

二、聯盟區塊鏈 (Consortium Blockchain): 此類區塊鏈的參與者並非都能獲的所有的資料，每個參與者會有不同權限，當進入區塊鏈之後會根據預先設定的規則驗證其身分而給予特定權限。所以此類區塊鏈是部分分散的架構。例如 R3 聯盟區塊鏈聚集全球 70 多個大型金融保險機構，使用半私有區塊鏈進行專案技術測試便是一例。[50]

三、私有區塊鏈 (Private Blockchain): 私有區塊鏈是以一個中央集中管理區塊鏈的使用權限，或是修改資料庫的權限。此類區塊鏈通常是納入組織的資訊系統中，以提供可加密稽核交易軌跡的好處。例如，集團企業可以使用私有區塊鏈讓該集團的不同子公司之間可以共享數據。[51]

### 第二項　區塊鏈在我國銀行業與保險業的運用

一、區塊鏈在銀行業的使用

[49] 同前註，頁 400，請參照「9.1.3 區塊鏈的類型與特性」章節中「一、區塊鏈的類型」有關公共區塊鏈的說明。

[50] 同前註，頁 400，請參照「9.1.3 區塊鏈的類型與特性」章節中「一、區塊鏈的類型」有關聯盟區塊鏈的說明。

[51] 同前註，頁 400，請參照「9.1.3 區塊鏈的類型與特性」章節中「一、區塊鏈的類型」有關私有區塊鏈的說明。



DOI:10.6814/NCCU202101656

台灣金融服務業在區塊鏈的應用以銀行業開始[52]。首先是富邦金控於 2016 年率先宣布要籌組區塊鏈金融聯盟，後來支持並成立台灣第一家商用企業區塊鏈公司 AMIS[53]。中國信託金控也宣布加入 R3 聯盟[54]並成立 50 人規模的實驗室。[55]國泰金控則是從自身集團業務中的主幹人壽保險為規劃，思考運用區塊鏈結合電子病歷來優化理賠作業。[56]玉山金控則是和國立台灣大學資工系在校園中完成區塊鏈行動支付的實驗。[57]而財金公司更是號召台灣金融保險機構共建區塊鏈平台。[58]

以富邦金控為例，台北富邦銀行在 2017 年 3 月就與政大合作簽約，進行「區塊鏈支付網路的關鍵技術與工程研發」專案計畫，9 月區塊鏈自行支付即獲得金管會核准，可進行商業運作，10 月份則開始進行銀行內部主機整合區塊鏈系統。[59]台北富邦銀行表示，整個專案花了半年時間即上線，並於 2018 年 4

---

[52] 沈庭安，區塊鏈跨產業應用現身，iThome，2016 年 10 月，https://www.ithome.com.tw/news/109176 ，最後瀏覽日：2021 年 9 月 1 日。

[53] AMIS 中文名稱為帳聯網路科技股份有限公司 (https://www.cakeresume.com/companies/amis?locale=zh-TW)，是一個實作及研究區塊鏈應用的軟體科技公司，目前產品主要有:數位資產保管服務、帳聯網、乙太坊研究及區塊鏈服務等。

[54] 參照「R3 聯盟 Corda 運行原理和優劣勢簡析」(https://www.chainnews.com/zh-hant/articles/706633449104.htm )，R3 又叫 R3CEV，C 即加密技術（Crypto），E 即交易所（Exchange），V 指風險投資（Venture），表明 R3 主要專注於以上三大業務。R3 於 2014 年創立以來，吸引了約 300 家全球知名銀行的加入，其中包括美國銀行、匯豐銀行、瑞銀等國際主流銀行。 R3 是一個全球性的商業銀行聯盟，Corda 就是這個聯盟的技術平臺。

[55] 張家嘯，中信銀布局金融區塊鏈國內首家 R3 聯盟成員，卡優新聞網，2016 年 10 月，https://www.cardu.com.tw/news/detail.php?nt_pk=26&ns_pk=30863 ，最後瀏覽日：2021 年 9 月 1 日。

[56] 沈庭安，前揭註 52。

[57] 同前註。

[58] 沈庭安，【打造臺灣最大銀行區塊鏈平臺】央行終於出手，財金公司串連國內 45 家銀行組區塊鏈平臺，iThome，2016 年 11 月，https://www.ithome.com.tw/news/109481 ，最後瀏覽日：2021 年 9 月 1 日。

[59] 李靜宜，臺灣第一個區塊鏈支付，台北富邦銀行在政大校園商家成立區塊鏈支付示範區，iThome，2018 年 5 月，https://www.ithome.com.tw/news/123145 ，最後瀏覽日：2021 年 9 月 1 日。



DOI:10.6814/NCCU202101656

月25日正式在政大開跑區塊鏈支付服務。台北富邦銀行2018年5月13日宣布，在政治大學推出區塊鏈支付應用場景，想要參與體驗的政大師生，可下載富邦行動銀行App，使用「Lucky Pay」掃描政大附近合作商家的QR Code後，即可完成付費。此舉讓台北富邦銀行成為臺灣首家提供可商業運作區塊鏈支付的銀行，而政大成為第一個區塊鏈支付示範區。「區塊鏈支付」是用區塊鏈的技術完成交易支付的流程。消費者感受不到 Lucky Pay 的背後，是使用區塊鏈技術完成清算、記帳，大家只會覺得這就是富邦銀行的「行動支付」。台北富邦銀行此次推出的區塊鏈支付服務，背後是由商用區塊鏈平臺公司 AMIS 所提供的區塊鏈技術，此技術是基於 AMIS 發表的新算法[60]，能夠大幅提升以太坊(Ethereum)[61]的訊息交換效率，將交易速度降至 1 秒以內，藉由這項技術，可以將區塊鏈應用到實際金融場景中[62]。

中國信託金控則是將區塊鏈技術應用於跨境匯款、貿易融資及智能保險等領域。自2017年起積極參與國內外重點組織，包括全球最大金融區塊鏈聯盟R3，旗下日本子行東京之星也加入SBI Ripple在日本的區塊鏈聯盟，與47家日本銀行合作建立下一代匯款平台。中信金在國內也是財金公司區塊鏈聯盟的成員，對於以太坊、 Hyperledger 等平台都有發展出可以支援的技術[63]。2018 年 1 月也

[60] 這裡所指的是「伊斯坦堡拜占庭 (Istanbul BFT)」演算法。該演算法的說明可以參照 Istanbul BFT 解讀(上)，https://www.gushiciku.cn/pl/pEag/zh-tw 。

[61] 請參照 CYBAVO「什麼是以太坊」(https://www.cybavo.com/zh-tw/knowledge-center/what-is-ethereum/)。以太坊（Ethereum）是一個開源的有智能合約功能的公共區塊鏈平台，通過其專用加密貨幣以太幣（Ether）提供去中心化的以太虛擬機（Ethereum Virtual Machine）來處理點對點合約。以太坊允許開發者在全局公共節點上運行分布式應用。

[62] 沈庭安，以太坊區塊鏈技術大突破，臺灣團隊 AMIS 創新區塊鏈共識演算，每秒交易量上看 1,200 筆，iThome，2017 年 7 月，https://www.ithome.com.tw/news/115341 ，最後瀏覽日：2021 年 9 月 1 日。

[63] 林弘斌、鄧介銘，淺談區塊鏈技術與金融區塊鏈實作驗證，財金資訊季刊，第 90 期，頁 21，2017 年 10 月。另參照翁芊儒，中信金控揭露未來區塊鏈戰略，聯手兩大國際組織，力推雙平臺瞄準內部金融應用與對外金流服務，iThome，2019 年 12 月，https://www.ithome.com.tw/news/134914。



DOI:10.6814/NCCU202101656

和區塊鏈音樂發行平台 Soundscape 合作，將中信的金流服務結合區塊鏈數位資產登記與轉移，讓 Soundscape 成為國內第一個擁有區塊鏈版稅結帳機制的音樂發行平台，成功將區塊鏈應用商轉[64]。2018 年 4 月再與陽明海運攜手，共同為客戶奇美實業完成國內首例區塊鏈國際貿易概念驗證，運用區塊鏈技術，加速海運及貿易融資流程，讓各貿易參與方節省二至四天的作業等待時間。利用區塊鏈技術不可竄改、不可否認、以共識機制達成同步帳本等特性進行概念驗證，由中信銀行同時提供進、出口商貿易融資服務，陽明海運則提供海運服務，與奇美實業共同完成由台灣出口至東南亞的交易流程[65]。效益上為加速整個國際貿易流程，節省進、出口商至少二天的作業等待時間; 銀行更可完整追蹤貿易進程，提升貿易融資產品的風險控管; 航運商亦能提升對提貨單據的掌握度，杜絕貨物被冒領的可能性並讓客戶更早取貨。

2018 年 2 月由金融研訓院、政大與 KPMG 三者主辦，成功完成保險理賠自動化、中小企業融資的區塊鏈 POC，透過智能合約(Smart Contract)[66]完成多項流程自動化、履約管理及透明化稽核等目標[67]。共有 6 家金融保險機構參與智能合約的研究。其中，國泰人壽、國泰產險加入保險自動理賠的研究。中小企業融

[64] 張庭瑜，音樂人的希望！台灣首個區塊鏈音樂發行平台 Soundscape 上線，數位時代，2018 年 1 月，https://www.bnext.com.tw/article/47772/kkfarm-soundscape-blockchain ，最後瀏覽日：2021 年 9 月 1 日。

[65] 中國信託新聞中心，中國信託、陽明海運與奇美實業三方攜手推出國內首例區塊鏈國貿概念驗證，2018 年 5 月，http://www.ctbcholding.com/file/news/2018/20180530.pdf ，最後瀏覽日：2021 年 9 月 1 日。

[66] 陳恭，智能合約的發展與應用，財金資訊季刊，第 90 期，頁 33-35，2017 年 10 月。智能合約是區塊鏈中一種制訂合約時所使用的特殊協議，主要用於提供驗證及執行智能合約內所訂定的條件。智能合約中內含了程式碼函式，亦能與其他合約進行互動、做決策、儲存資料及傳送以太幣等功能。這些交易具有可追蹤、難以竄改與不可逆轉的特性，使智能合約能在沒有第三方的情況下，仍能進行安全的交易。此外，智能合約由創建者定義、由區塊鏈網路執行所建構而成，其當中與合約條款相關的所有訊息，全都是按照合約當中所設定的操作自動執行。

[67] 沈庭安，保險理賠與企業融資 2 大智能合約 POC 驗證達成，安侯建業與政大聯手研發區塊鏈應用，iThome，2017 年 3 月，https://www.ithome.com.tw/news/112796 ，最後瀏覽日：2021 年 9 月 1 日。



DOI:10.6814/NCCU202101656

資方面的研究則有華南銀行、第一銀行、元大金控以及土地銀行。採用以太坊的私有鏈架構，儲存保險理賠的紀錄以及貸放款記錄，並將智能合約導入其中[68]。在中小企業融資平台方面，以智能合約降低資產交易的媒合成本，中小企業融資更公開、透明，讓閒置資金的人可以找到投資對象，需要資金的人也可以找到金主。架構上以區塊鏈為主，再串接鏈外的系統。因為採以太坊的私有鏈的機制，因此可以進行會員驗證。同樣的，也是將智能合約應用在貸放流程中的管理。使用智能合約的部份包含了融資案的申請與管理、實體資產與數位資產的同步、區塊鏈內與區塊鏈外系統整合、融資案管理（分割數位資產、圈存投資）、債權管理(智能合約可以自動、定時的進行期中扣款、還本息以及逾期警示)、稽核軌跡。

二、區塊鏈在保險業的使用

國內的保險業對於區塊鏈的使用保全/理賠聯盟鏈的建立和智能合約的自動理賠服務。

自 2019 年起保險業在業界共識與主管機關樂觀其成的態度下，開始進行「保全/理賠聯盟鏈」的專案，希望未來能達成單一契約變更或是理賠申請時，文件可以共通的目標[69]。該專案所為遵循的法律基準包含「保險業申請業務試辦作業要點」、「保險法」、「個人資料保護法」、「保險業辦理電子商務應注意事項」及「金管會指定非公務機關個人資料檔案安全維護辦法」。

在保全聯盟鏈方面，主要由壽險公會負責區塊鏈資料傳輸系統維運，而險

[68] 同前註。

[69] 李靜宜，【保全理賠聯盟鏈政策推手：金管會保險局長施瓊華】資料共享，讓民眾和業者能雙贏，下一步要所有保險公司都加入，iThome，2020 年 8 月，https://www.ithome.com.tw/news/139137 ，最後瀏覽日：2021 年 9 月 1 日。



DOI:10.6814/NCCU202101656

種上先以限定個人險保單並排除團險及待記名式保單，也限人身保險契約的要保人保全變更申請[70]。個人資料的變更包含姓名、身分證統一編號、地址、電話及電子郵件信箱。參與試辦的業者共計 11 家，其中包含壽險業 9 家及產險業 2 家。保全鏈的模式是當保戶有參與保全聯盟鏈的保險公司保單需要進行個人資料變更時，只須向參加保全聯盟鏈的其中一家透過公司網站、APP 或是金融服務業務員的行動裝置提出申請，並簽署保全申請轉送暨個資蒐集同意書後，同意由首家保險公司透過聯盟鏈傳送相關資料，經由壽險公會所維運的保險區塊鏈聯盟科技運用共享平台雲端服務(所謂的主共識節點)使用區塊鏈技術進行加解密傳輸及傳輸資料紀錄，將所變更的資料同時對其他加入保全鏈並持有該保戶保單的同業進行更新。更新後首家保險公司及轉收保險公司均會對保戶發出資料變更申請已經受理的通知。由壽險公會所主導的雲端服務平台，是由中華電信所提供的雲端服務為建構基礎，所有聯盟參與者都在這樣的架構之下使用該平台進行資料的傳輸與驗證。這樣的雲端架構算是一種具特定使用目的及對特定成員開放的公有雲。較一般公有雲的範圍是比較限縮的。

而理賠聯盟鏈與保全聯盟鏈在業務流程概念與雲端服務架構上大致相同，但是因為理賠的處理較為複雜且與保戶權益有相當關係，所以理賠聯盟鏈開始在險種上是以限定個人險保單，排除團險及待記名是保單，並且限定是健康險或傷害險的醫療保險金給付(但不含旅平險)。同時在給付金額和領取方式上也有限制。在流程上是當保戶透過行動 APP 或是網站申請理賠時，除檢附理賠申請所需文件及影像資料外，也須簽署「理賠申請轉送暨個資蒐集同意書」。相關資料隨即由首家保險公司進行處理，首家保險公司確認理賠申請文件無誤後會將相關申請資訊與影像傳送至壽險公會所負責維運的區塊鏈資料傳輸平台，並

[70] 李靜宜，【保險公司不再是數據孤島】聯盟鏈將開啟資料共享新時代，iThome，2020 年 8 月，https://www.ithome.com.tw/news/139136 ，最後瀏覽日：2021 年 9 月 1 日。



DOI:10.6814/NCCU202101656

通知轉收保險公司理賠申請文件均已到位。轉收保險公司透過區塊鏈的加解密技術檢視傳送資料的傳送狀態。當資料符合相關資安規範後，即接收理賠申請資訊與影像，接著通知受益人理賠已經受理。若所提供文件經審理無誤後即可進行核賠作業。保戶不再需要與所投保之各保險公司逐一提供理賠文件進行申請，只需啟動理賠聯盟鏈的其中一家即可使其他加入聯盟鏈的保險公司同時處理相關理賠作業，相當便利。

在企業自行使用區塊鏈的使用是關於智能合約在理賠自動化方面[71]。理賠自動化的目標是減少申請、紙本作業的繁雜流程，靠區塊鏈智能合約簡化保險理賠。保險理賠中，以現有系統為主，區塊鏈為輔，並將部分保險合約轉成智能合約，並且利用共享帳本的特性，有權限地分享 保險理賠的申請記錄。智能合約被運用在「履約保險」，負責執行智能合約以實現自動化理賠的流程。「計算理賠金額」是根據醫療資訊、保險理賠規則來計算相應的保險費用。「金流管理」藉由智能合約自動化的把資金轉到保戶或醫院。「稽核軌跡」利用智能合約收集區塊鏈上的行為用以稽核。國泰金控旗下的國泰產險，則是攜手安侯企業管理股份有限公司(KPMG)，將個人旅行綜合保險承保範圍中之班機延誤部分，導入區塊鏈並結合智能合約，針對航班預訂抵達與實際抵達目的地之時間資訊予以比對，於確認符合班機延誤理賠條件時，主動理賠，提供保戶更優質的服務[72]。此保險科技(InsurTech)針對旅行綜合保險中之班機延誤部分，整合航班資訊查詢功能，將保戶於要保時提供之航班資料，搭配智能合約自動檢查班機抵達目的地時間、延誤條件等，透過區塊鏈可追蹤、不能修改之特性，於確認保

[71] 李顯正，前揭註 41，頁 411，請參照「9.2.3 區塊鏈在保險業的應用實例」章節中「一、智能合約(Smart Contract)之自動理賠」有關智能合約在保險理賠中的優點說明。

[72] 國泰金控，國泰產險攜手安侯企管運用保險科技創新技術結合區塊鏈與智能合約 提供班機延誤主動理賠，資訊中心，https://www.cathayholdings.com/holdings/information-centre/intro/latest-news/detail?news=h14I3VgFLEmpT5xZbswwhA ，最後瀏覽日：2021 年 9 月 1 日。



DOI:10.6814/NCCU202101656

戶所搭乘航班延誤並符合理賠條件時，國泰產險除將主動通知保戶外，保戶只需提供相關理賠文件，國泰產險即可依約給付賠款，大幅提升理賠處理效率與強化對保戶之服務[73]。

智能合約的技術運用可以視為區塊鏈的加值型產物。在已經有聯盟鏈的情況之下，透過智能合約的技術服務，可以將保險理賠的服務更加自動化與透明化。而這類整合企業內部系統與企業外部系統的技術架構目前是以私有雲為主的服務平台並與外界的系統介接，外部系統提供會啟動自動理賠的相關資訊，例如航空公司的航班資訊或是天氣資訊等，而保險公司以私有雲的方式處理關於智能合約的相關資訊，因為這部分是主管機關所認定包含個資需高度控管的機敏性資料，並以聯盟鏈的方式處理理賠業務，私有雲在與外部系統介接時必須有較多重的資訊安全保護機制，例如多層防火牆架構、系統使用者權限控管及非軍事區(Demilitarized Zone, DMZ)網段設計等方式才能提供較多的保障。

### 第三項　小結

本節說明銀行業與保險業在使用雲端服務中有關區塊鏈的成果。銀行業利用區塊鏈的技術發展區塊鏈支付、區塊鏈結帳、跨境匯款、融資貿易與智能合約等金融服務。保險業利用區塊鏈發展自動化理賠的智能合約、保全/理賠聯盟鏈。以上這些區塊鏈的發展都與雲端服務有關。要將區塊鏈的特性發揮，透過雲端服務是較為可行的做法，因為這兩者都是以網際網路為基礎的科技。銀行業對於區塊鏈的使用應該會以聯盟鏈為基礎進行如銀行間的結算業務，或是國際貿易的匯兌業務，以及跨業結盟的行動支付或結帳的業務。保險業也會擴大目前已經形成的保全/理賠聯盟鏈，提高保險業的參與度，在未來完成保單電子

[73] 陳恭，前揭註 66。



DOI:10.6814/NCCU202101656

化以及類似證券集中化管理的機制後，將可以明顯提升客戶服務的品質。另外若智能合約能達成標準化，對於保險業在業務擴展上也會有助益。

## 第三節　我國銀行業與保險業運用雲端服務和巨量資料處理

### 第一項　巨量資料處理說明

巨量資料又可稱為大數據(Big Data)，是指巨型資料的集合。這資料集合的大小通常超出人類在可以接受的時間下收集、使用、處理和管理的能力[74]。巨量資料處理的目的，是將大量的資料集合用以滿足多樣性、不同目的與不同速度的需求。多樣性是指資料結構有傳統性的交易資料及非傳統性的資料，例如影像、聲音、社群媒體活動紀錄等。不同目的則是指對資料的蒐集、儲存、分析或是比對。不同速度則是指對資料的定時批次、及時查詢等。達到巨量資料等級的資料量，多半為 TB (terabyte)等級的資料集合。雲端服務的興起帶動巨量資料處理，因為提供雲端服務的廠商可以提供足夠的資源來滿足巨量資料處理的需求，包含儲存空間及運算能力。而一般企業受限於 IT 資源的投入規模，必須借重雲端服務的資源才能進行[75]。

可稱為巨量資料者，一般歸納有四大特性: 大量性 (Volume)、多樣性 (Variety)、時效性 (Velocity)和真實性 (Veracity)。以上四大特性便是一般所稱的

---

[74] Villanova University, What is Big Data? https://www.villanovau.com/resources/bi/what-is-big-data/ , last visited: 1st Sep 2021。另參照 INSIDE，巨量資料的時代，用「大、快、雜、疑」四字箴言帶你認識大數據，https://www.inside.com.tw/article/4356-big-data-1-origin-and-4vs，參照大數據(Big Data)的說明:「或稱巨量資料 ，顧名思義，是指大量的資訊，當資料量龐大到資料庫系統無法在合理時間內進行儲存、運算、處理，分析成能解讀的資訊時，就稱為大數據。」.

[75] 黃正傑，前揭註 26，頁 11-1，請參照「11-1-1 巨量資料處理技術的概念」關於巨量資料與雲端服務的關係說明。



DOI:10.6814/NCCU202101656

「4V」。

一、大量性 (Volume):

所要處理的資料量大。資料大量產生是巨量資料的主要特徵。資料量大的定義需視個案狀況而定，有可能是每筆資訊精簡但數量龐大的交易資料，也有可能是每筆包含複雜影音資訊但數量並非關鍵因素的分析用資料。資料的性質與數量均會決定是否構成巨量資料的條件[76]。

二、多樣性 (Variety)

資料的多樣性一般指的是同時包含結構化與非結構化的各種資料型態。結構化資料一般來自於應用系統中所記錄與儲存的資料，多半可以儲存於關聯式資料庫系統中且資料的邏輯性十分明確，邏輯的嚴謹度亦高。半結構化的資料多半來自如掃描文件、電子郵件或是網頁等資料。非結構化資料多數指來自社群網站、影像、聲音等。混合處理結構化與非結構化的資料而找出具有商業價值的資訊是巨量資料處理的主要任務[77]。

三、時效性 (Velocity)

處理不同時間需求的資料是巨量資料處理的特徵。有些以月份、季別或年度為時間刻度的資料處理，會是以批次方式於一定時間內將整包資料做分析而得到結果，如月報表、季報表或年報。有些為即時資料分析，例如像購物網站

[76] 同前註，頁 11-2，請參照「11-1-1 巨量資料處理技術的概念」關於巨量資料特性中大量(Volume)的說明。

[77] 同前註，頁 11-2，請參照「11-1-1 巨量資料處理技術的概念」關於巨量資料特性中多量(Variety)的說明。



DOI:10.6814/NCCU202101656

根據客戶的查詢而將同性質商品或是相關性商品同時提供於客戶所瀏覽的網頁中，對於客戶提供即時的行銷訊息[78]。

四、真實性 (Veracity)[79]

真實性意味著可靠度。當資料來源變的多元時，資料來源的品質與可靠性是影響巨量資料處理結果的關鍵。所以巨量資料在處理前對於來源資料正確性需控制，分析並過濾資料中有偏差、偽造或異常的部分，這樣對於巨量資料處理的結果才具可信度[80]。

綜合上述，我們可以說稱巨量資料者須同時具有這四大特性，因此在進行巨量資料處理時，要能先辨別哪些資料來源是有意義的資料來源，接著透過可靠有效的資料分析方法，才能萃取出有用的結論，進而有助於決策的執行[81]。

關於巨量資料的處理流程，一般分為以下六階段:

一、資料採集階段

此階段為資料蒐集的初始階段，一般來說是透過既有與顧客接觸管道，蒐集並儲存各種顧客習慣及行為資料，例如在企業網站瀏覽的內容、消費購物的喜好、以及 Cookies 所記錄的資料，將收集到的數據存放在原始資料庫中，供下

[78] 同前註，頁 11-2，請參照「11-1-1 巨量資料處理技術的概念」關於巨量資料特性中速度 (Velocity)的說明。

[79] 廖文華、張志勇、蒯思齊，前揭註 4，頁 82，請參照大數據的五 V 特性。

[80] INSIDE，前揭註 74，參照真實性的說明。

[81] 吳啟彰，巨量資料 (Big data)產業應用成功的關鍵在於速度，不在巨量!，管理知識中心，2015 年 11 月，https://mymkc.com/article/content/22243 ，最後瀏覽日：2021 年 5 月 23 日。



DOI:10.6814/NCCU202101656

一階段使用[82]。

二、資料整理階段

資料在採集時具有多源及多樣性、質與量均存在差異，在彙整資料庫進行巨量資料分析前，需要進行資料整理，從大量的資料中，篩選出有用的資料。資料整理是實現巨量資料處理價值的關鍵。[83]

三、資料儲存與管理階段

巨量資料最具前瞻性的發展方向，是整合不同來源、多方向的數據，提供全方位的商業行為預測功能。而管理方式會決定資料的儲存格式，儲存格式則影響資料分析的深度與廣度。在資料儲存與管理上，除須兼顧結構性、半結構性與非結構性的數據外，供分析使用之數據，其深度與廣度是強化資料有效性很重要的一環[84]。

四、資料分析階段

將已經完成整理階段的資料運用適當的工具或方式進行分析，分析的目的必須清晰並建立分析的規則，將資料依規則進行分類、排序、關聯性分析，最後建立結論。分析的過程中，在深度上宜將新、舊資料相結合，在廣度上則宜

[82] 朱啟恆，大數據於金融業之應用，財金資訊季刊，第 84 期，頁 14，2015 年 10 月。請參照「(一)數據採集」。

[83] 同前註，請參照「(二)數據清整」。

[84] 同前註，請參照「(三)數據儲存與管理」。



DOI:10.6814/NCCU202101656

包含結構性及非結構性的資料[85]，並採用即時性分析以符合時效性[86]。

五、資料採礦(data mining)階段

資料採礦的目的在於從資料中提取隱藏其中、過去未知的潛在有價值訊息，經由統計與分析等層層的整理及歸類，將巨量資料轉化成商業行為的預測，以及具有商業價值的趨勢預測，並因應分析目標的不同需求，建構出新的業務模式，協助企業制定明智且切實可行的策略[87]。

六、商業應用階段

巨量資料的價值要能落實成實際的行動才能真正實現，通過前述五個階段的處理，巨量資料處理從分析過去所發生事情的規律中，挖掘出新的業務模式，供決策者將其轉換成可執行的方案，有利於推動業務發展，贏得競爭優勢[88]。

巨量資料處理需要使用大量的 IT 資源，如伺服器與儲存設備以及適合的分析軟體，這樣龐大的 IT 費用支出對於中小型企業是較大的負擔，對於不常使用巨量資料分析的大型企業也是不必要的投資，因此以雲端服務的方式提供巨量資料處理會成為前述企業的選擇[89]。但是當巨量資料處理所使用的資料有屬於個人資料的類型時，就必須考慮到巨量資料處理使否和於所蒐集資料的目的及

[85] 黃正傑，前揭註 26，頁 11-2，請參照「11-1-1 巨量資料處理技術的概念」關於巨量資料特性中多量(Variety)的說明，「結構化的資料可能是傳統的 ERP、CRM、銷售點資訊系統(POS)紀錄等關聯式資料庫資;半結構化資料可能來自文件、電子郵件、網頁等資料;非結構化資料則來自於社群網站、影像、聲音等資料。

[86] 朱啟恆，前揭註 82，請參照「(四)數據分析」。

[87] 同前註，請參照「(五)數據挖掘」。

[88] 同前註，請參照「(六)商業應用」。

[89] 黃正傑，前揭註 26，頁 11-5，請參照「11-1-1 巨量資料處理技術的發展」，其中「二、發展趨勢」對於雲端服務是巨量資料處理的發展趨勢之一有相關說明。



DOI:10.6814/NCCU202101656

資料當事人是否同意的議題。

## 第二項　巨量資料處理在我國銀行業與保險業的運用

### 一、巨量資料處理在銀行業的使用

銀行業是財務資料生產、倉儲、處理及傳輸的集合， 而運用巨量資料分析去預測客戶需求，發展更貼近客戶需求的經營模式，是銀行業使用巨量資料處理的主要目的[90]。巨量資料處理於銀行業的應用，可分為四大類：

#### (一) 客戶關係管理

銀行業的客戶包含個人及企業，而個人資料包括人口統計學特徵、消費能力、興趣、風險偏好等；企業客戶資料則包括企業的生產、流通、運營、財務、銷售、相關產業鏈上下游等。好的客戶關係管理會同時使用銀行業自身業務所採集到的資料以及整合外部更多的資料，如：客戶在社群媒體上的行為資料、客戶在電子商務網站的交易資料、企業所在的產業鏈上下游外部環境發展情況的資料等，以擴展對客戶的瞭解[91]。

#### (二) 精準行銷

在建立客戶關係管理基礎上，銀行業可以展開各種業務行銷措施，例如根據客戶的即時狀況進行行銷；或根據客戶交易紀錄分析以便就不同業務或產品進行交叉推薦；也可以根據客戶的年齡、資產規模、理財偏好等，對客戶群進

[90] 朱啟恆，前揭註 82，頁 15，請參照文中所引用麥肯錫公司 (McKinsey & Company) 所公布的「大數據的下一個前沿：創新、競爭和生產力」報告中的結論與作者的說明。

[91] 同前註，頁 16，請參照「(一)客戶關係管理」。



DOI:10.6814/NCCU202101656

行精準定位，分析出潛在需求，或使用客戶行為分析結果，發展針對性的客群行銷策略等，以提升經營績效[92]。

(三) 風險管理

銀行業須建構健全的風險管理機制體系做為營運上的責任負擔。各類風險管理均須持續執行並及時反應，以降低營運上的風險。一般銀行業所面臨的市場風險、信用風險、作業風險及流動性風險，可根據多年來所建置的客戶相關資訊進行風險分析，量化客戶的信用額度，藉此提供客製化貸款條件以滿足客戶的需求。另外金融服務業在進行國內外金融商品的投資時，亦可運用大數據分析將投資組合的風險控管予以最佳化。在有效預防與管理金融犯罪上，巨量資料分析所得的客戶消費行為模式，藉由即時詐欺交易識別與分析，當發現不正常消費時，可立即得知並採取行動，在短時間內找出盜用者，以便及時遏阻銀行因盜用事件所可能蒙受之損失[93]。

(四) 優化服務

通過巨量資料處理，金融服務業可追蹤各種市場的變化，將客戶行為資料透過所建立的資料分析模組中，綜合客戶的資產特徵、風險偏好、金融往來習慣等，進一步預測客戶潛在的需求，將精準行銷擴展至服務的創新與優化[94]。

目前我國銀行業在巨量資料分析的投入與應用上可以提供參考的有:國泰金控設立數位數據暨科技發展中心（簡稱「數數發」）協助全集團進行數位轉型[95]。

---

[92] 同前註，頁 16，請參照「(二)精準行銷」。

[93] 同前註，頁 17，請參照「(三)風險管理」。

[94] 同前註，頁 17，請參照「(四)優化服務」。

[95] 王宏仁，國泰金控如何打造數據生態系？核心架構和關鍵戰略大公開，iThome，2019 年 10



DOI:10.6814/NCCU202101656

玉山銀行成立資料科學團隊來分析全臺灣數百家分行，根據各區域擬定不同的經營策略[96]。合作金庫銀行建置 360 度客戶視圖，作為打造自家資料驅動決策的基礎，目標是未來銀行內各部門都能以數據分析或視覺化數據成果，管理並訂定業務發展策略，並將數據資料落實為戰略資產[97]。中國信託銀行成立數據暨科技研發單位（簡稱數研發），達成搶攻數位金融的新藍海，以 AI(Artificial Intelligence)[98]確保金融大數據應用落地、並以數據掌握顧客人生不同階段需求，提供超級個人化服務，並用 Digital First 結合全通路體驗，作為與純網銀競爭關鍵[99]。上述範例各有其對於巨量資料處理所欲達成的目標雖有其不同的商業考量，但其建置的原則仍是大致相同。以下僅以國泰金控的實例為說明。

國泰金控的數位轉型方向一開始就聚焦數據和技術來協助全集團轉型。國泰金控旗下除了銀行，還有人壽、產險、證券、投信和創投等子公司，顧客總數將近 1,300 萬人。數數發中心主要團隊，有以數位服務、產品開發和設計為主的 Digital Team，包括了數位行銷團隊、數位體驗設計團隊、數位平臺開發人力等。另一團隊則是 Data Team，任務是從資料中使用新興科技，如大數據、雲端、機器學習，來協助業務開拓。Data Team 旗下又設有資料科學實驗室（Data Science Lab），專門研究最新的資料科技或 AI 技術[100]。在大數據分析的導入上，資料團隊以 FAST（Flexibility、Agile、Scenario 和 Trust）原則，建立一套彈性

月，https://www.ithome.com.tw/news/133440，最後瀏覽日：2021 年 5 月 23 日。

[96] 王立恆，要靠數據尋找分行營運新機會，玉山資料科學團隊經驗大公開，iThome，2016 年 10 月，https://www.ithome.com.tw/news/108614，最後瀏覽日：2021 年 5 月 23 日。

[97] 李靜宜，合庫靠數據驅動數位轉型，要讓資料變成關鍵戰略資產，iThome，2020 年 9 月，https://www.ithome.com.tw/people/140102，最後瀏覽日：2021 年 5 月 23 日。

[98] 李顯正，前揭註 41，頁 344，請參照「人工智慧的定義」。

[99] 李靜宜，中國信託銀行瞄準新金融時代 3 大機會，將靠 AI、超級個人化以全通路迎戰純網銀，iThome，2020 年 10 月，https://www.ithome.com.tw/news/140577，最後瀏覽日：2021 年 9 月 1 日。

[100] 王宏仁，前揭註 95。



DOI:10.6814/NCCU202101656

的數據平臺架構，從資料輸入到輸出的資料分析流程來設計分為四層，包括資料層（Data Layer）、線上產品層（Online Production Layer）、線下產品層（Offline Production Layer）和探索層（Exploration Layer）[101]。資料層包括了顧客資料、線上數位資料、外部資料以及來自不同產業的資料等，而線上產品層則有各種面對顧客的通路服務，網站上的數位行為機制，或是自行開發的網路爬蟲服務，還有各種資料服務。線下產品層則主要是資料處理流程的中後段，除了傳統的 ETL(Extract-Transform-Load)[102]處理和資料倉儲系統之外，數數發還建置一套資料湖(Data Lake)，資料湖的資料還可以提取出來進行不同的 ETL 處理，再匯入資料倉儲或資料湖中，反覆循環再利用，另外在線下產品層中，還有一個關鍵的模組就是分析平臺，可以快速套用資料團隊建立的各種 AI 模型來進行分析。探索層則包括了一套可以進行探索性分析的平臺。後三層之間，彼此都可以透過應用程式介面(Application Programming Interface, API)串連。這套架構不只可以應用到傳統的資料處理流程，資料蒐集後，儲存到關連式資料庫中，進行 ETL 處理，集中到資料倉儲，再進行後續利用，還可以彈性搭配不同用途。目的是打造一套可以自由組合由程式化控制和自動串接的資料服務架構[103]。

這套架構整體上是以私有雲為基礎而建置的。主要考量是為達到未來的目標:「資料即服務 (Data as a Service, DaaS)」架構[104]。DaaS 架構分為三層，最下

[101] 同前註。

[102] ETL 是 Extract-Transform-Load 三個字的縮寫，是建置或更新資料倉儲中的內容時，對於所需之數據進行資料擷取、轉換、載入的過程。Extract 是資料擷取：從資料來源處擷取所需之數據資料。Transform 是資料轉換：針對所擷取出之數據資料，依照商業邏輯的需求，針對數據資料作適當的轉換。Load 是資料載入：最後將已作適當轉換過的數據資料載入到目的地。可參照 https://www.netpro.com.tw/?FID=23&CID=82&category=1 說明。

[103] 王宏仁，前揭註 95。

[104] 同前註。



DOI:10.6814/NCCU202101656

層是數據資料架構的基礎建設，中間層則是先進技術層，主要提供各種數據分析模組，例如統計分析、AI、機器學習[105]、深度學習[106]、自然語言處理(Nature Language Processing, NLP)、Data API、推薦系統、風險分析、數位分析等都屬於 DaaS 中間層，而最上層是場景實踐，主要目的是達成「人機協作」，透過技術和機器來輔助人的作業，這一層目前的成果包括了即時決策系統(Real Time Decision Management, RTDM)、ROBO 智能投資服務、阿發智能客服 Chatbot、RPA(Robotic Process Automation)流程機器人等[107]。以此為目標的架構設計之下，技術上使用大量開放性元件(Open Source)是因為需要處理許多來源不同及格式多樣的資料，系統開發上也採取 DevOps[108]的設計架構暨軟體工程概念以配合所謂微服務(Micro Service)[109]的彈性，長期規劃上更有將與公有雲的結合變成混和雲的型態納入考慮，所以先建置私有雲的大數據平台架構。這樣的規劃安排也是基於法規監理的考量，因為目前巨量資料的處理受到個資法的規範及主管機關的高度監督管理，因此銀行業多半還是自建處理中心為主，藉以完整掌握資料處理的透明度及資訊安全的完整度。當法令上的調整使公有雲服務業者可以參與銀行業的巨量資料分析業務時，採取混和雲的方式進行合作將會是主要的模式。

[105] 李顯正，前揭註 41，頁 346，請參照「機器學習(Machine Learning)」。

[106] 同前註，請參照「深度學習(Deep Learning)」。

[107] 王宏仁，前揭註 95。

[108] DevOps 為英文 Development (開發) 和 Operation (運營) 的縮寫組合。Development 指的是軟體開發，Operation 主要指的是技術運營＆維護，可以視為軟體開發、技術運維及品質保障 (Quality Assurance, QA) 的交集。請參照 Sindy Chen，DevOps 介紹 》建立 DevOps 文化，消除開發、營運、品保斷層，CakeResume，https://www.cakeresume.com/resources/what-is-devops?locale=zh-TW，最後瀏覽日：2021 年 6 月 20 日。

[109] 鄭淳伊，走入軟體架構演進史見證微服務發展今昔，網管人，2019 年 4 月，https://www.netadmin.com.tw/netadmin/zh-tw/technology/1716C14FB29749B68D8E74C93ACA6263 ，最後瀏覽日：2021 年 9 月 1 日。



DOI:10.6814/NCCU202101656

## 二、巨量資料處理在保險業上的使用

保險業在巨量資料處理的應用上算是起步較晚，多半是跟隨著金控集團或是銀行業的腳步前進。國際研究暨顧問機構 Gartner 全球金融服務產業研究與諮詢部門副總裁暨分析師 Kimberly Harris-Ferrante 在她的觀察中明白指出[110]「保險產業擁抱新興科技的步調，通常比整體金融產業晚 2 到 3 年。」。Gartner 的報告中指出，以目前在越來越多元的新興資訊技術中，對於保險產業而言，AI 是最具潛力與轉化型力量的新興科技，足以打造更個人化的客戶體驗。以保險業前端的應用來說，能透過 AI 訓練過的聊天機器人、理財機器人，讓保險產品的線上銷售與服務流程更加完整，提升客戶體驗；而在保險業後端，也能使用 AI 提高承保、理賠的處理效率，進而降低整體成本。保險產業整體價值鏈都可運用 AI，包括行銷、銷售、保險產品定價與承保、保單發予、服務理賠流程、營運等 6 個部分都能使用到。而巨量資料的處理、分析與利用就是 AI 的前端[111]。

壽險業中的中國人壽，自 2017 年起開始進行數位化轉型，而轉型的主要策略就是從大數據來建構 AI 的戰略布局[112]。首先透過開發行動投保 APP 的方式使業務人員在第一時間可就以蒐集、處理和利用客戶資料，完成保險手續的相關作業。前端透過行動 APP 架構的 i-Agent 平台，後台的資料處理上則建立起 AI 智能標籤庫，將本來就已經在資料庫裡的客戶理賠、異動、契約變更等資訊善加利用，透過 AI 技術進行大數據分析，找出客戶潛在需求與意圖動向，並把 AI 標籤產生在客戶身上。目前中壽已經有 70～80 個智能標籤，客戶的資料一進來，

---

[110] 李靜宜，Gartner：數位轉型腳步雖慢，但不出 5 年，AI 將成為保險業主流應用，iThome，2018 年 5 月，https://www.ithome.com.tw/news/123542，最後瀏覽日：2021 年 9 月 1 日。

[111] 同前註。

[112] 李靜宜，中國人壽揭露數位轉型戰略，靠 AI 打造業務員最強武器，iThome，2019 年 6 月，https://www.ithome.com.tw/people/131411，最後瀏覽日：2021 年 9 月 1 日。



DOI:10.6814/NCCU202101656

進行快速分析後，就能用 AI 自動貼標。這些貼在客戶身上的 AI 標籤，都將透過中壽開發的行動投保平台 i-Agent，隨時提供給業務員以輔助他們掌握客戶最新情報，在適當的時機提供客戶可能需要的服務。而中壽分析資料的來源，除了客戶原始的保單資料，也會去檢視客戶是否在中壽做過契約變更，例如，變更地址、電話、或是繳別（如從年繳保費變為月繳保費）等。此外，資料來源也包括客戶在中壽網站的瀏覽行為，例如是否瀏覽過健康險頁面等。採用了 AI 自動貼標，就是要讓產出標籤的時效性與未來可應用部分能夠快一些回應。關於大數據分析在中長期的發展還包含 AI 建模、人臉辨識、人工智慧理賠防詐系統，以及推出為業務員打造的智能助理。以中國人壽的需求來看，要能符合將大數據分析與行動科技相整合，並且未來可以提供多項 API 串接應用的技術架構，非雲端運算莫屬[113]。但就現階段相關法令對於雲端科技在金融服務業應用的規範，以私有雲的方式建置是較務實的做法。尤其未來有可能與保全或是理賠聯盟鏈的結合考量，以私有雲為主再輔以相關界接的公有雲所建構的混和雲應當是在整合效益和成本上較佳的選擇。

在台灣以電話行銷為主要業務管道的美商康健人壽，於 2019 開始進行數位化轉型。首先在組織調整上成立數位洞悉部門專責大數據的分析，IT 部門專責系統環境改造與巨量資料分析相關技術的提供。康健人壽的整體資料處理有兩大來源，第一類為電銷系統所蒐集保戶相關資料，該資料的規模為康健人壽在台灣設立子公司開始約 30 年的保戶與保單相關資料，另一類為康健網路投保平台[114]的保戶及官網註冊會員的相關資料。面對歷史資料的巨量性與新型態資料的結構多樣性，IT 部門開始進行基礎建設的調整，除了在硬體建構上延續並擴大以虛擬機為核心的超融合架構外，在系統開發與管理上開始導入 DevOps 的平

[113] 同前註。

[114] 李曇純，我國保險科技的發展，東吳大學法律學系碩士論文，頁 37-41，2018 年 6 月。



DOI:10.6814/NCCU202101656

台，引進較多樣的工具以便對於多樣性的資料可以進行更彈性的處理，對於大量資料的梳理與整合也透過導入 ETL 的工具進行更有效率的處理。這些調整就是以打造康健人壽的私有雲為目標。巨量資料的處理往往在需求上會有不確定性，這樣的不確定性對於 IT 資源的配置是一項挑戰，無論是在運算資源或存儲資源上的提供都是如此，IT 部門的任務除了提供巨量資料處理所需的服務外，更大部分的工作是在維持企業內各資訊系統的正常運作。在考量企業對 IT 的預算支出下，能夠靈活彈性的運用 IT 資源是企業在數位化轉型的過程中能否順利的關鍵，而私有雲的建立正式這個議題的最適當解決方案。如之前所述關於巨量資料處理的六階段，其中與 IT 部門有密切關係的是資料採集、資料整理、資料儲存與管理，而接下來的資料分析、資料挖掘與商業應用就是數據洞悉部門的課題。目前較具體的成果有提供電銷人員成交機率較高的銷售名單、網路註冊會員的行銷活動建議及異常理賠案件的警示。現階段康健人壽在大數據的應用上大多為資料批次作業後的分析研究，未來將朝向及時銷售與客戶服務的目標邁進。

### 第三項　小結

本章對於我國銀行業與保險業在巨量資料處理的運用現況上做說明。巨量資料處理需要使用大量的 IT 資源，但是巨量資料處理的商業綜效是需要時間即持續投入才會逐漸顯現。所以雲端運算的架構對於剛開始發展巨量資料處理的企業而言是進入門檻較低的解決方案。我國銀行業與保險業對於這方面的發展已經從嘗試性階段邁入實作性階段，可以從客戶服務、精準行銷、風險管理等方面獲得回饋。因為銀行業與保險業所處理的巨量資料與個人資料有關，為符合監理機關對於個人資料保護的要求，目前多半是用私有雲的架構在發展，隨著法規的調整，利用公有雲的資源優勢與現階段已建置完成私有雲結合的混合雲應該是下一階段的方向。另外對於巨量資料處理的內容如有關於個人資料時，



DOI:10.6814/NCCU202101656

需要對於個人資料使用是否超過原來蒐集的目的及是否獲得資料當事人同意等個人資料保護法上的議題進行檢視。

## 第四節　我國銀行業與保險業運用雲端服務與資訊管理

### 第一項 資訊安全

雲端運算在資訊安全上也可以提供相關的服務，這就是安全即服務的概念(Security as a Service, 簡稱 SaaS。與 Software as a Service 的簡稱相同)[115]。雲端型態的安全即服務有兩種: 第一種是現有的資訊安全廠商將其產品由原本在地形式轉換成透過雲端遞送的服務，改變以往提供於網路、主機或應用系統的主從式架構，例如 Symantec, Trend Micro 等;另一種是由雲端服務廠商與資安業者合作直接提供資安服務，如 Akamai。以上兩種方式的興起，都與資安攻擊日趨複雜化與巨量化有關。愈來愈多的資安攻擊事件顯示攻擊者或是入侵者都以具規模性、計畫性和技術性的方式進行。除了惡意的攻擊之外，垃圾郵件也造成企業在維運上的困擾。企業在面對這些資安議題時，直接的方式是加強企業自身資訊基礎建設的防禦能力，以維護企業系統及營運的正常。但是這對企業來說是人力物力上無止盡的成本投入，常常陷入資安風險承擔與資安措施做到何種程度的困難抉擇。再加上資安防護日趨專業，企業本身在人員的訓練與培養上也未必可以及時發揮效果。所以將部分資訊安全作業委外日漸成為趨勢。

目前資安即服務所提供的內容可分為以下幾項:

---

[115] 黃正傑，前揭註 26，頁 14-17，請參照「14-4 資安即服務」說明，指提供企業或雲端服務業者以較低的成本取得專業資安管理的服務。



DOI:10.6814/NCCU202101656

一、身分認證與存取管理

將身分認證與存取權限管理透過雲端服務方式進行，以便使用者可以跨企業內部系統進行作業。同時提供各種認證及存取失敗紀錄，成為日後稽核作業的輔助資料[116]。

二、資料洩漏保護

監控和保護企業內部資訊系統、雲端服務項目、使用者端的資料存取狀況和資料傳輸等，以避免未經授權的使用或是資料的遺失[117]。

三、網站安全性確保

提供企業在最前端的網站安全性保護。主要是將所謂的DMZ直接建置於雲端服務上，透過雲端服務的防衛機制來避免企業網站因受到攻擊而服務停擺或是被竄改及植入惡意程式[118]。

四、電子郵件安全性確保

電子郵件的安全包含釣魚信件的過濾、附件檔案的安全性偵測、以及郵件傳遞與公司資安政策合規性處理、重要郵件加密等。另外關於垃圾郵件的阻擋過濾通常也納入該項服務的範疇[119]。

---

[116] 同前註，頁 14-18，請參照「1.身分認證與存取管理服務」說明。

[117] 同前註，頁 14-18，請參照「2.資料洩漏保戶服務」說明。

[118] 同前註，頁 14-18，請參照「3.網站安全服務」說明。

[119] 同前註，頁 14-18，請參照「4.電子郵件安全服務」說明。



DOI:10.6814/NCCU202101656

五、安全性評估

企業的應用系統與軟硬體環境隨著營運發展而日趨複雜，定期的弱點掃描及安全性合規檢測亦日趨重要。雲端服務可以在檢測的時效性及頻率上提供更有效率的作法[120]。

六、入侵偵測與入侵防禦

為防止對企業外部網站進行惡意地入侵或滲透，尤其是進階持續性滲透攻擊 (Advanced Persistent Threat, APT)，雲端資安服務會透過入侵偵測系統(IDS, Intrusion-detection system)或是入侵防衛系統(IPS, Intrusion Prevention System)來加以預防及反制[121]。

七、軌跡紀錄與資安事件處理

無論是網路、伺服器、系統應用程式等，都會留下相關活動或交易的軌跡，這些紀錄的保存與不可被竄改的特性是需要特別的設備或程式加以維持。雲端安全的服務可以提供較為彈性的作法。另外也可以針對 IT 維運所發生的事件進行紀錄和警示，也可以產生統計報表[122]。

八、加密與金鑰管理

資料進行加密的演算法會隨著演算法的複雜度而影響加密的速度與資源使用。機敏性資料的加密可以藉由雲端服務來提供較新及較具效率的加密流程。

---

[120] 同前註，頁 14-18，請參照「5.安全評估服務」說明。

[121] 同前註，頁 14-18，請參照「6.入侵偵測服務」說明。

[122] 同前註，頁 14-18，請參照「7.資訊安全與事件管理服務」說明。



DOI:10.6814/NCCU202101656

此外對於加解密所需的金鑰，雲端服務也可以提供適合的管理方式[123]。

九、業務持續營運與災害復原

營運持續與災害復原都是在 911 事件之後為企業所重視的資安議題。以往需要由企業自行準備相關軟硬體設備，而今藉由雲端業者所提供的服務，可以在成本效益與資安需求上達到平衡，從系統還原、資料備份以及最後的營運持續皆可以用較具彈性的作法達成其目標[124]。

十、網路安全

從網路設備及各節點的運作狀況，到網路流量的監控。從企業內部到雲端，這些皆可以由安全及服務的雲端方式解決。尤其是對於阻斷服務攻擊(Distributed Denial of Service, DDoS)的網路攻擊，目前實務上已經是從 Gb 級的攻擊量為基本規模，相信 Tb 級的攻擊應該很快就會是常態。面對這樣的趨勢，企業若是使用雲端資安的解決方案，相信可以將這種攻擊行為所產生的影響降低至最小[125]。

目前在台灣金融服務業最常談論的雲端資安服務，應屬網路安全。較為典型的個案是 2017 年證券商集體遭受 DDoS 的攻擊事件[126]。2017 年 1 月台灣股市封關之後，有證券商在年假期間就出現了第一起的 DDoS 攻擊事件，2 月股市開市後部分證券商在開盤後即遭受 DDoS 攻擊。攻擊者大都挑選早上 8 點和 10 點

[123] 同前註，頁 14-18，請參照「8.加密服務服務」說明。

[124] 同前註，頁 14-18，請參照「9.持續營運管理與災害復原服務」說明。

[125] 同前註，頁 14-18，請參照「10.網路安全服務」說明

[126] iThome, 臺灣史上第一次券商集體遭 DDoS 攻擊勒索事件，iThome，2017 年 2 月，https://www.ithome.com.tw/news/111875 ，最後瀏覽日：2021 年 9 月 1 日。



DOI:10.6814/NCCU202101656

之間的時段，鎖定券商發動洪水式 DDoS 攻擊。攻擊對象呈現隨機，造成證券商網站下單系統無法提供正常的服務，而駭客勒索最多 10 個比特幣，並揚言不付款將進一步發動 Tb 等級攻擊，駭客主要是利用 NTP 攻擊這些證券商的服務系統，少部分還會利用其他服務協定發動攻擊，如 SNMP、TFTP，這是台灣史上第一次券商集體遭受 DDoS 攻擊勒索的事件。企業與主管機關共同配合採用多層次縱深防禦的處理方式來因應，包括將攻擊流量導入中華電信所建置的雲端「清洗防護區」，並進行攻擊模式樣本比對過濾，透過利用阻擋、隔離、清洗流量方式，來幫助券商用戶有效緩解DDoS攻擊。並強化網絡營運中心(Network Operation Center, NOC)/安全營運中心(Security Operation Center, SOC)資安監控，也提升網路端點的資安防護能力，最後順利抵擋住這一次的攻擊行為。

至於其他的資安服務，金融服務業因為考量管理上的主控性與主管機關的監理查核，並對於機敏性資料或是控管方式與權限等因為在雲端服務內運作的細節與疑慮尚未完全釐清，所以大多仍在評估階段。

### 第二項 資料存儲

雲端服務中關於資料存儲是對多數企業較具吸引力且進入門檻較低的服務選項。雲端儲存是一種網路線上儲存的模式，即把資料存放在雲端服務提供者的多台虛擬伺服器，而非專屬的伺服器上。雲端業者營運大型的資料中心，有資料儲存代管需求者，則透過向其購買或租賃儲存空間的方式，來滿足資料儲存的需求。雲端服務提供者根據客戶的需求，在後端準備儲存虛擬化的資源，並將其以儲存資源池（storage pool）的方式提供，客戶便可自行使用此儲存資源池來存放檔案或物件。實際上，這些資源可能被分布在眾多的伺服主機上。雲端儲存這項服務乃透過 Web 服務應用程式介面或是透過 Web 化的使用者介面



DOI:10.6814/NCCU202101656

來存取[127]。

雲端儲存是一種雲端運算模型，透過以服務形式管理和操作資料儲存的雲端運算供應商將資料存放在網際網路上。它以隨需方式交付，提供適時的容量與成本，無須購買和管理自己的資料儲存基礎設施且獲得「隨時、隨處」資料存取的靈活性、全球擴展和耐用性。因此主要的優點為企業只需要依實際使用的儲存空間支付費用給雲端服務業者，不需要自建實體的儲存裝置，可減少資訊設備的支出和管理成本，日常維運工作(如備份、資料複製、或是增加儲存裝置等工作) 也可轉移給雲端服務提供者，讓企業更可以專注在核心業務上[128]。

儘管雲端存儲有前述的好處，但仍有對於雲端存儲的疑慮，首先是安全性。對於個人資料的儲存與管理，一直是雲端存儲被關注的重點，這其中包含存放的位置與方式、資料管理的方式和資料使用者與資料管理者的權限控管等問題，因為雲端服務是資源池共享的概念，資料處理流程和儲存方式(如資料處理的中繼站有哪些、資料儲存的共享方式和所在地等)，一直是雲端服務的灰色地帶，缺乏明確的說明。其次雲端存儲因為是靠網路做遠端的資料存儲，所以網路傳輸的優劣會影響資料存儲的可靠性與可用性，尤其當資料需要即時更新或是巨量傳輸時，網路品質所產生對資料品質的影響是不容忽視的。而且就資料存儲效能上來看，在地端的存儲效能一定是優於遠端的存儲效能。最後是監理上的困難度，當主管機關有特定的資料使用軌跡的要求時，雲端服務業者是否能配合提供所需的軌跡是一項變數。

綜合上述，銀行業與保險業對於公有雲所提供的雲端存儲在使用上仍較為

[127] 廖文華、張志勇、蒯思齊，前揭註 4，頁 100-102。

[128] AWS，雲端儲存，https://aws.amazon.com/tw/what-is-cloud-storage/ ，最後瀏覽日：2021 年 9 月 1 日。



DOI:10.6814/NCCU202101656

保守。關於雲端存儲的案例，可以參考美商康健人壽的做法。康健人壽為了因應 IFRS17[129]全球性會計準則的適用，將亞太區有設立子公司的國家如泰國、印尼、新加坡、馬來西亞、台灣、澳洲等財務資料進行統整，以期望達到亞太區各子公司未來在提報各項財務資料時可以有一致性的資料型態，同時總公司在進行財務分析時也有共同基準的報表規格。因為是從各個不同地區的資料彙整至單一處理中心，所以採用 AWS 的 PaaS 服務架構，利用雲端資料存儲，各國子公司分別將財務資料上傳至康健人壽在 AWS 新加坡資料中心所建立的資料池，再透過康健人壽在亞太地區的專案團隊使用雲端應用程式平台開發相關程式進行資料的梳理作業。各國上傳的資料在當地均先完成去識別化的處理後才進行上傳。對於跨國企業而言，雲端服務在特定業務需求上的確有其必要性，因為就效率及成本的考量上是適當的選擇。目前國內金融服務業的作法，大都是用超融合架構(Hyper-Converged Infrastructure, HCI)[130]為主建構私有雲來做初步資料存儲的雲端化，替未將資料處理作業與公有雲結合預做準備。

### 第三項 IT 部門的轉型

IT 部門的轉型可以從兩方面來說明:雲端服務的模式及雲端服務的架構。雲端服務的模式包含 IaaS、PaaS、SaaS 三種類型，這三種類型代表不同程度 IT 業務的委外模式，其中 IaaS 的委外程度最低，其次是 PaaS，而 SaaS 的委外程度最高。當 IT 部門使用雲端服務進行業務委外後，業務重心會逐漸從例行性維護作業例(如系統更新、老舊設備汰除及過時技術的升級等)移轉至科技管理與廠

[129] 勤業眾信 Deloitte，《新準則》IFRS 17：保險合約，2017 年 5 月，http://www.ifrs.org.tw/IFRS/NewInfoPDF/N081.pdf ，最後瀏覽日：2021 年 9 月 1 日。

[130] 張明得，什麼是超融合架構？，iThome，2016 年 1 月，https://www.ithome.com.tw/tech/102114 ，超融合基礎架構（Hyper-converged infrastructure，縮寫爲 HCI），是一種整合了儲存裝置及虛擬運算的資訊基礎架構框架。在這樣的架構環境中，同一廠商的伺服器與儲存等硬體單元，搭配虛擬化軟體，被整合在一個機箱之中。



DOI:10.6814/NCCU202101656

商管理的作業。科技管理的聚焦會是替組織提供適合的資訊技術來達成商業目標並對於組織的科技架構發展制定藍圖和計畫。廠商管理會以選擇適當的廠商及確保廠商的服務品質為主。這樣的轉變會使 IT 部門越來越貼近公司業務的決策層級並參與更多討論，傳統上多半是業務單位決定業務發展方向然後 IT 單位提供技術支援，但未來 IT 單位可以根據科技趨勢發展、同業科技運用及科技廠商評鑑等主動提供對公司業務方向的建議[131]。

雲端服務的架構為公有雲、私有雲、混和雲及社群雲。當 IT 部門在導入雲端架構時，要先確認那些服務或系統可以轉換成雲端架構。若使用公有雲架構時，是要將現有的系統移轉至公有雲或是將新的系統建置在公有雲，IT 部門需要評估系統移轉的可行性與資料安全及隱私的保障。IT 部門要能評估這些面向，就需要有公有雲端架構的專業知識，因此要對 IT 人員進行教育訓練。若是自行建置私有雲，IT 人員也需要對私有雲的架構特性和技術學習，將現有系統整合並移轉至私有雲架構所需要考量的因素與移轉至公有雲相比是範圍較小些，但是需要增加對於雲端架構管理的知識和技能，因為私有雲的管理是由 IT 自行負責而非廠商。藉由對於雲端架構的了解，IT 部門的人員在專業知識的領域上也會轉變。IT 人員在系統維運雲端化的帶動之下，工作上將會著重於如何有效率從雲端服務中選擇和搭配可以供企業在達成營運目標上的資訊系統解決方案，或是以新的技術與觀念將既有的系統做效能及功能上的優化或配合商業策略做新系統架構的轉型。還須注意是在資訊安全及合規的要求上，雲端服務的資安管理方式亦不同於原來在地化的資安管理方式，所以資安政策修正、資安相關作業辦法的調整、以及相關稽核和監理的作業方式，都需要做同步的配合。所

[131] Tim Mather, Subra Kumaraswamy, Shahed Latif，胡為君 譯，前揭註 32，頁 236-237、264-265。



DOI:10.6814/NCCU202101656

以雲端業務的導入對於 IT 部門角色上的轉型將會是必然的結果[132]。

台灣目前銀行業與保險業大都已先自建私有雲為起步。建立私有雲可以視為 IT 部門雲端化的初期階段。私有雲的建立也是依照雲端服務的原理來導入，先進行 IT 資產與系統的盤點與整併達到 IT 資產輕量化的目標，接著基礎建設的部分採用超融合和虛擬化的技術將原本分散的軟硬體轉置於虛擬化的架構中，使用相關工具進行網路、伺服器、存儲設備等做彈性化的資源管理。應用系統也同時建構在虛擬化的環境中，使用相關的開發工具及管理工具進行程式開發和更新。同時導入 DevOps 的流程觀念，使應用系統生命週期的管理更為自動化和具有效率。同樣在資訊安全的管理上也會因為這樣的變動而配合調整。這些做法也都使 IT 部門的角色進行轉變。前述提到關於國泰金控或中國信託銀行在區塊鏈或是巨量資料處理等個案，都可以看出 IT 部門在運用雲端服務後發生組織內的轉型。

[132] iThome，面對雲端運算，資訊部門該怎麼做?，2010 年 12 月，https://www.ithome.com.tw/node/65236，最後瀏覽日：2021 年 9 月 1 日。



DOI:10.6814/NCCU202101656

# 第三章　銀行業與保險業運用委外雲端服務的資訊安全與個資議題

本章對於銀行業與保險業在運用委外雲端服務上的資訊安全和隱私權相關議題進行說明。首先是對委外雲端服務的一般資訊安全風險做說明。其次，因為銀行業與保險業有其特殊性，對於資訊安全的要求標準較其他行業更高，所以在運用委外雲端服務上的資訊安全議題須另外補充。委外雲端服務在銀行業與保險業共同的個資議題也會在本章中提到，最後會從保險業的營運環節角度來說明運用委外雲端服務的個人資料保護議題。

## 第一節　銀行業與保險業運用委外雲端服務的資訊安全風險

### 第一項 委外雲端服務的一般資訊安全風險

企業對於是否該採用委外雲端服務的考量中，資訊安全的風險一直都是主要的因素。根據雲端服務的架構不同，所需要考量的因素也會有強度上的差異。一般而言，私有雲的資訊安全問題多半仍在企業內部的資安控管領域之中，所以會是以企業本身資安的政策及原則來處理。而公有雲或是混和雲的架構就比較複雜，因為外部的因素介入較多，資訊安全的議題較為多元[133]，所以會是本論文主要觀察的對象。公有雲端服務(例如 Google GCP, Amazon AWS, 微軟 Azure 等)的一些主要特性，例如跨地域性與大規模的網路存取、資源的集中與共享、以及多樣性雲端服務的連結和堆疊，使得企業在評估委外雲端服務時對於該服

[133] 劉定基，雲端運算與個人資料保護-以台灣個人資料保護法與歐盟個人資料保護指令的比較為中心，東海大學法學研究第 43 期，頁 93-96，2014 年 8 月。



DOI:10.6814/NCCU202101656

務所具備資訊安全水準的周延性與明確性都持審慎的態度。綜觀雲端服務所帶來的主要資訊安全風險主要有以下幾點:

一、外部使用者的惡意行為

雲端服務業者為了增加客戶數量，常常會提供各類優惠以降低使用門檻，同時也放寬對客戶條件的評估及審查標準。這樣的做法會讓具有惡意的使用者以簡便的程序或方法取得公有雲中價值較高的服務，然後透過這些服務進行雲端系統的入侵，再用木馬程式植入或殭屍電腦佈署等方式利用雲端系統廣泛連結與分享的特性，達到更大的破壞行為[134]。

雲端服務的最大優勢之一，就是提供資源共享的軟硬體環境，同時也提供技術上的一致性與標準化，其目的就是讓使用者群可以共同分攤 IT 資源的成本，並以使用者付費的概念做有彈性的使用[135]。但是共享資源的環境如果沒有作適度的環境區隔和資安控管，便會提供有心者入侵他人資料庫或是應用程式的管道。這個風險對於企業是否要使用公有雲端服務或是要如何使用，都是一個需要釐清的課題。

二、不安全的軟體或 API

公有雲的三種服務類型: SaaS, PaaS 和 IaaS 都會提供許多應用軟體或具外接服務性質的介面程式 (Application Programming Interface, API)作為雲端服務使用者可以串接或是擴張使用範圍的方法。但是有些開源軟體 (Open Source Application)因為發展的成熟度尚未完備，可能會產生一些資安上的漏洞; 而 API

[134] 黃正傑，前揭註 26，頁 14-2。另參考前揭註 4，12-4 雲端運算的資安管理，頁 274-276。

[135] 同前註，頁 14-3。



DOI:10.6814/NCCU202101656

的部分同樣也會有資安漏洞的問題。除此之外，公有雲的服務可以利用 API 對於其他的雲端服務產生串接以擴大服務的功能，但是各串接的雲端服務在資安管理的標準上參差不齊，所以這樣的運用也會有資安的風險[136]。

三、雲端業者內部人員的惡意行為

公有雲端業者內部人員的控管機制，包含資安管理規範的執行、職務與工作的權限區分和控管、內控內稽的強度等，都是對於內部人員管理的重要環節。而這部分的資訊通常屬於雲端業者的內部資訊，雲端客戶通常較難監督和評估，因此對於雲端業者的內部管以是否達到應有的資安管理水準而足以避免內部人員的惡意行為，是使用雲端的企業疑慮[137]。

四、資料遺失或外洩

雲端服務對於資料的管理基本上也是遵循資料的建立、儲存、使用、分享、保存、清除的生命週期來進行各階段的管理。這些過程中都有可能會因為操作不當、設備失靈或是惡意行為而造成資料的洩漏或滅失。公有雲端服務對於資料管理政策的周延性，將會影響資安風險的評估[138]。

五、使用者帳號的盜用

使用者帳號容易因使用端的管理欠周延而遭到像是釣魚方式、社交工程、程式猜測攻擊或側錄使用行為等手法而被竊取進而盜用。一但公有雲端服務遭

[136] 同前註，頁 14-3。

[137] 同前註，頁 14-3。

[138] 同前註，頁 14-3。



DOI:10.6814/NCCU202101656

受這一類的資安威脅，因為其雲端服務的共享資源特性，容易造成的資安危害風險會比原本企業自建私有雲的模式要來的更高。這也是公有雲端服務風險較高的原因[139]。

六、其他未知的風險

公有雲端服務因為其複雜度高，因此服務提供廠商多半只提供原則性的說明，無論是架構技術面、資源管理面和資訊安全的執行方式都是如此。服務使用者在實務上很難對其運作進行監督或評估，因此對這部分的防護措施多半也只能較被動的配合公有雲端服務業者。這種低度自主性的委外管理，會使服務使用者無法適度掌控資安風險的評價，因而將資安風險暴露在不確定性的狀況中，這是公有雲在資安風險考量上較高的原因[140]。

## 第二項 銀行業與保險業委外雲端服務的資安議題

我國金融服務業對於委外雲端服務的資安風險除前述所提的一般性風險之外，由於產業屬性特殊，還需要將其他的風險因素納入觀察。以目前進入 Bank 4.0[141]時代金融業所累積及使用巨量金融資訊與數據，外加已經開放的純網銀及未來開放銀行(Open Banking)的趨勢帶動下[142]，高效率與高質量的數據運算將是

[139] 同前註，頁 14-3。

[140] 同前註，頁 14-3。

[141] 「銀行 4.0 啟動三零革命」，BIG DATA FINANCE，說明「銀行 1.0」是指以分行為主要客戶通路的傳統銀行；「銀行 2.0」是自助銀行設備出現，讓銀行在打烊後，還能提供服務；銀行開始使用 ATM，並在 1995 年因網際網路開始商業化而加速；「銀行 3.0」是智慧手機於 2007 年出現，愈來愈多交易轉移到行動支付、P2P 等現象；「銀行 4.0」是透過技術會隨客戶所需即時提供內建的、無所不在的銀行服務，這種服務由即時的、情境式參與的體驗、無障礙的互動，並由 AI 的建議層主導；絕大多數都透過數位全通路，完全不需要實體營運據點，很像是「純網銀」，https://bigdatafinance.tw/index.php/finance/bank/755-4-0 ，最後瀏覽日：2021 年 9 月 1 日。

[142] 李靜宜，金管會公布 2020 年 FinTech 施政重點：開放銀行新階段、數位帳戶未成年開戶、保險區塊鏈上路、純網銀下半年開業，iThome，2020 年 1 月，



DOI:10.6814/NCCU202101656

不可避免的需求。在現今的科技環境中，雲端運算確實能夠提供這個趨勢的解決方案[143]。但考量資訊外移至第三方儲存、處理及運用時資訊安全的確保程度，與在金融產業監管的架構下，銀行業與保險業將部分服務內容委託第三人處理的做法，必須符合相關法令規定。除前述一般公有雲常見的資安問題外，而當屬於高度監理的銀行業與保險業在評估公有雲的服務時，則會以更嚴格的標準來衡量。銀行業與保險業向來掌握大量客戶的資料，受到個人資料保護法及相關法令規範，也因此對於資安風險會有更深一層的考慮。

綜合而言，我國金融服務業在使用第三方雲端服務的資安風險考量主要有以下幾點:

一、容許性:金融監理機關態度與法令的變更

金管會對於金融服務業使用公有雲的服務一直以來都採取嚴格審查的態度。不過這也是因為公有雲服務的相關技術在初期並未十分完善，資安的措施也無法滿足主管機關在監理上的要求，因此無論是金融業或是政府機關都對第三方的雲端服務存有觀望的態度。但隨著近幾年來資訊科技與資安技術的日新月異，許多以前技術上的限制逐一被克服，金融業開始重新考慮第三方雲端服務所帶來的優點，並不斷呼籲監理單位應該要與時俱進的審視雲端服務的進步現況並適度放寬金融業使用雲端服務的規範。

為回應產業界的需求及推進金融科技發展，金管會經過二場公聽會後，於2019 年 6 月 27 日公告發布「金融保險機構作業委託他人處理內部作業制度及程

https://www.ithome.com.tw/news/135363，最後瀏覽日：2021 年 9 月 1 日。

[143] 王宏仁，銀行開放上雲端的衝擊不只金融圈，而是將臺灣雲端產業做大了，iThome，2019 年 6 月，https://www.ithome.com.tw/voice/131522 ，最後瀏覽日：2021 年 9 月 1 日。



DOI:10.6814/NCCU202101656

序辦法」（委外辦法）部分條文修正草案，針對金融服務使用雲端科技將制訂明確的法律權源及相關管理辦法，使金融保險機構得使用雲端科技提供金融服務同時兼顧消費者權益保障，於修法正式通過後即得正式上線[144]。但未來隨著實務上運用第三方雲端服務所產生的問題，或是國際間對於個人資料保護、資訊安全要求及洗錢防制或反資恐等國安議題的法規調整，金融監理機關對於現行法令再做限縮的調整也是有高度的可能性，伴隨而來會是金融業對於使用第三方雲端服務所要達到的資安或個資保護規範的難度應該會愈來愈高。主管機關一旦進行法令進行修改，金融業在使用委外雲端服務的作業上勢必要有相對的回應，有可能需要收回原本在委外雲端上的業務項目，或是對於資安管理的強度要投入更多資源。這種不確定性是金融業欲使用委外雲端服務時的風險因素。

二、對委外雲端服務的風險評估

金融機構因為擁有大量客戶資料且決定蒐集資料的類別與利用目的，在個資法中被視為資料控管者(data controller)的角色是無庸置疑的。在使用第三方雲端服務時，雲端服務提供者則可能被視為個資法中的受託者，但關於資料保護的實際權責仍在資料管理者[145]。因此，對於受委託的第三方雲端業者需要進行風險評估並且進行適當的風險控管是金融機構無可迴避的責任。但是因為第三方雲端業者通常可以提供的維運資訊或是服務細節會基於商業機密考量而有所限制，所以使用服務的金融機構如何能完整的評估委外雲端服務的風險會是一個重要挑戰。在確認委託雲端服務風險的前提之下，才能針對確認出的風險擬定對應的控管機制以降低其發生的機會和發生時的處理方式，這是一個連動性

[144] 廖婉君，廖婉君觀點：金融科技服務躍上雲端的資安挑戰，風傳媒，2019 年 7 月，https://www.storm.mg/article/1467059?mode=whole ，最後瀏覽日：2021 年 9 月 1 日。該辦法最近一次修訂為中華民國一百零八年九月三十日依據金融監督管理委員會金管銀外字第 10802725940 號令修正發布第 7、12、13、19、21 條條文；增訂 19-1、19-2 條條文。

[145] 劉定基，前揭註 133，頁 84-85。



DOI:10.6814/NCCU202101656

的關係。但是目前這部分的資訊透明度不夠清晰，所以是需要評估的風險。此外，委託機構對於所要委外業務的性質與重要性也需要評估該業務在委外後的風險，包括欲委外業務對於營運的重要性及佔全體業務的比重程度，委外業務是否過度集中於單一雲端業者等都是資安風險評估的因素。

三、最終監督義務、實地查核及第三方查核

依照金管會目前對於金融服務業使用委外雲端服務的相關委外辦法來看，金融機構對於委外雲端服務業者仍負有最終監督義務。基本上就是個資法施行細則第 8 條的概念展現[146]。根據個資法施行細則第 8 條，委託機關與受託機關的區別在於委託機關有權決定個人資料之蒐集、處理、利用及資料的範圍、類別目的和期間，而受託機關僅能在委託機關預設的範圍內，實際進行資料的蒐集、處理、利用。所以銀行業與保險業在使用委外的雲端服務時，還是要承擔對客戶個人資料保護的最終責任，並對受託的雲端業者負擔最終的監督義務。因此委外雲端業者對於資料的儲存、資料存取控管、資料備份方式都會是委託的金融機構在個資保護的檢視點。基本上就是回歸到委外雲端業者資源共享概念之下，是否可以更清晰透明的呈現出對個別委託機構在作業面上的區隔，這也是對委外雲端服務風險高低的衡量方式之一。對金融機構來說，明確清晰的作業細節、獨立區隔的實體區間、控管機制嚴密的作業流程等會使資安風險降低。但這些要求與委外雲端服務業者的配合能力或許不相當，這也是資安上的風險。

金融機構也面臨另一個資安風險，就是如何對於委外的雲端業者進行資安查核。這從兩個角度來觀察，第一是查核的方式，第二是查核的結果。關於查

[146] 個資法施行細則第 8 條參照。



DOI:10.6814/NCCU202101656

核的方式，依照金管會的要求，金融機構在與受委託的雲端業者簽訂委託契約時，契約內容是要保有金融機構本身、主管機關或中央銀行等可以取得受委託雲端業者的相關資訊及實地查核的權利[147]。從查核方式來說，如果雲端服務提供相關設備環境及軟硬體均在國內，實地查核執行的問題比較不大。但是如果委外雲端業者的相關服務設備部分在國境之外時，實地查核就會遇到一些挑戰。如果是由委託的銀行或保險機構自身去執行實地查核可能還可以執行，但是如果是主管機關或是其他公務機關執行時，這就會關係到各國管轄權與公權力跨境監督管理的議題，因此在執行層面上可能會相當困難。

另外，關於查核結果的評價也是一個需要關注的面向。因為委外雲端服務具有高度技術面與作業面的專業性和複雜性，所以進行查核時，委託的銀行或保險機構本身是否有足夠的查核能力來進行查核作業是需要考慮的。如果沒有具雲端服務的專業查核能力，對於資安風險的確認便會有不完整的問題[148]。當然，目前法令是允許金融機構可以委託具備資訊專業的第三方進行查核作業，但是第三方的查核範圍及應具備資格能力，均應符合法令規定[149]。金融機構本身對於這樣的查核結果是否有評價的能力也是一個需要考量的風險。不過委託專業第三方查核的方式或許可以成為前述主管機關對實地查核要求的替代方案

[147] 金融監督管理委員會，預告「金融機構作業委託他人處理內部作業制度及程序辦法」部分條文修正草案，https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=201906270002&dtable=News ，最後瀏覽日：2021 年 5 月 25 日。

[148] 花俊傑，雲端法規遵循與稽核建議，網管人，2012 年 5 月，https://www.netadmin.com.tw/netadmin/zh-tw/technology/7B41372FD1CA4316A8366E50EF111C77 ，最後瀏覽日：2021 年 9 月 1 日。

[149] 金融監督管理委員會，預告「金融機構作業委託他人處理內部作業制度及程序辦法」部分條文修正草案，https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=201906270002&dtable=News ，最後瀏覽日：2021 年 5 月 25 日。



DOI:10.6814/NCCU202101656

[150] 。

四、資料加密與金鑰保管

在委外雲端服務與個人資料保護的討論上，資料加密機制一直是重要的議題。有關資料加密的面向有兩個，一個是資料「傳輸時」的加密機制，另一個是資料「存儲時」的加密機制。委託雲端服務的主要服務骨幹就是網路的傳輸，尤其是以網路進行資料的傳輸為其核心。傳輸方面的加密機制可以分為傳輸「方式上」的加密及傳輸時將「檔案」加密兩種形式。所謂傳輸方式上的加密一般係指使用具加密機制的通訊協定(protocol)來完成，如 SFTP[151], FTPS[152], HTTPS[153]等，這是屬於一種端點對端點的加密方式，被視為網路層的加密。但是光只有網路層的加密並不一定能保證資料的完整性(即不容竄改性)，因此更為嚴謹的做法是發送者將檔案加密後再進行傳輸，而收件者於接收檔案並且解密後再進行資料後續的處理。資料傳輸時的加密是可以確保資料從寄件者送出到收件者接收之間資料的保密性和完整性。

至於資料儲存時的加密，以雲端服務的類型來觀察，IaaS 的服務類型在資料儲存時提供加密機制是較為可行的，某些類型的 IaaS 服務，例如僅以委外雲端服務當作資料異地備分環境的需求時，委託者的資料就像是以單純貨物倉儲的方式存放於受託雲端服務者的環境之中，資料並不會在雲端的環境中進行使用，而是當有需要時再回傳至委託者自己的資訊系統環境中，所以對資料進行

[150] 同前註。

[151] Stanley Hui，[Day24] 資料傳輸安全(通道加密)，iThome，2017 年 1 月 https://ithelp.ithome.com.tw/articles/10188645 ，最後瀏覽日：2021 年 9 月 1 日。

[152] 同前註。

[153] The Economic Times，Definition of 'HTTPS', https://economictimes.indiatimes.com/definition/https, last visited: 1st Sep 2021.



DOI:10.6814/NCCU202101656

加密不但可行而且應該是必要的。不過如果委外雲端服務的使用方式不是僅限於資料的存放，而是做到資料的處理，就會發生因資料加密而產生應用系統效能上的瓶頸。關於 PaaS 和 SaaS 的服務類型，由於這兩種委外雲端服務都需要在雲端環境中進行應用系統上的運作並且進行資料處理，因此儲存的資料若加密則將導致資料在搜尋及處理上的困難，也會使委託者在雲端上所維運的應用系統功能受到限制。但是如果在委外雲端服務的資料沒有加密機制，雖然雲端業者均聲稱其內部在作個別客戶的資料區隔時都會有不同的資料標籤(data tagging)而避免資料的誤用[154]，此外若是有使用者利用惡意程式侵入其他使用者應用系統的弱點而進行資料的竊取或是竄改，勢必成為個資保護上的隱憂。目前針對委外雲端服務的資料加密議題，已經嘗試利用同態加密(homomorphic encryption)[155]的技術來處理。委託者可以透過同態加密的技術將加密過後的資料上傳雲端後，在雲端環境中不須經過資料解密而對已經加密的資料進行運算，運算的結果傳回委託者端進行解密後與未加密的資料運算結果一致。使用同態加密的資料處理方式可以避免加密資料因為在委外雲端環境處理時需暫時性解密而產生的資料外洩風險，並且達到資料處理的目的。同態加密技術目前的限制性是在運算的效能，這種較複雜的加密技術對於電腦資源的消耗性較大，同時在運算的時間上也會比較長，因此對資料處理做靜態的分析用途(如巨量資料分析)較適合，若是要做動態及時的資料處理(如即時互動式的智能客服)則還需要一段時間發展。

---

[154] Tim Mather, Subra Kumaraswamy, Shahed Latif，胡為君 譯，前揭註 32，頁 55。

[155] 參考「同態加密 – 區塊鏈技術指南」，https://poweichen.gitbook.io/blockchain-guide-zh/crypto/homoencryption，定義為:「是一種特殊的加密方法，允許對密文進行處理得到仍然是加密的結果。即對密文直接進行處理，跟對明文進行處理後再對處理結果加密，得到的結果相同。從抽象代數的角度講，保持了同態性。」關於同態加密的近期發展可以參考「Google 開源完全同態加密軟體工具」，iThome，2021 年 6 月，https://www.ithome.com.tw/news/145102 ，最後瀏覽日 2021 年 9 月 1 日。



DOI:10.6814/NCCU202101656

再者，與加密機制息息相關的金鑰保管也是一個重要議題。雲端服務的金鑰管理方式，與傳統金鑰管理方式的原則並無不同，其考量的重點包括了金鑰的儲存保護、金鑰的存取控制及金鑰的備份與還原[156]。金鑰的管理方式應與其他敏感資料的管理方式一樣，因此金鑰在傳輸、存放、備份時都需要受到妥善的防護，尤其是金鑰的儲存地點要避免和加密資料位於相同的儲存媒體，以免連帶性的災難同時發生導致資料無法還原。哪一個主體可以取得並使用金鑰是金鑰存取控制實施的重點，為了限制只有特定的主體才可使用，採用強度高的身分驗證機制和職務角色的分離，都可以預防發生不當的資料存取事件。金鑰一旦遺失也就表示著資料再也無法解密，所以針對經過加密的重要資料，必須建立其安全的金鑰備份機制[157]。承前段所提關於雲端服務的類型不同，金鑰保管的方式也會不相同。通常 IaaS 的服務類型金鑰可以由委託的金融機構自行保管，雲端業者只需負責對已經加密好的資料做好保管的措施即可。但是當使用 PaaS 或是 SaaS 型態的服務時，金鑰的保管機制就會變得比較複雜。如果金融機構使用委外雲端業的金鑰管理機制，就意味著金融機構本身對於金鑰的管理亦委託雲端業者而處於低度控管的狀態。這樣的方式對於金融機構而言是具相當風險性的，因為委託方無法確知自己所使用的金鑰是否與其他客戶分享。理想的金鑰管理方式還是應該由委託人自己掌控金鑰的產生、管理與保存，所以前述同態加密因為可以滿足這樣方式，預期將可成為委外雲端服務上廣泛使用的技術[158]。

[156] Tim Mather, Subra Kumaraswamy, Shahed Latif，胡為君 譯，前揭註 32，頁 180-181。

[157] 花俊傑，雲端資料加密與金鑰管理，網管人，2012 年 11 月 https://www.netadmin.com.tw/netadmin/zh-tw/technology/0D7370C1E5DC41F59827A3538CC08A85，最後瀏覽日：2021 年 9 月 1 日。

[158] 陳奕廷，輕量加密、同態加密與區塊鏈：新世代密碼學的三大聖杯，科學 Online，2018 年 8 月，https://highscope.ch.ntu.edu.tw/wordpress/?p=79164，最後瀏覽日：2021 年 9 月 1 日。



DOI:10.6814/NCCU202101656

五、資料所有權

金融機構與委外雲端服務業者在儲存資料上的關係，仍是由金融機構掌控資料而受委託的雲端服務業者僅能在受託業務範圍之內執行，而不可以進行範圍以外的利用。因此對於金融機構所委託雲端業者儲存或使用的資料，金融機構必須有完全的所有權。但這個議題的困難點在於如何確保金融保險機構有完全的所有權。理論上還是需要透過金融保險機構完全掌控資料加密、金鑰管理與存取權限控管等資料管理方式來降低資料被未經授權使用的風險。並且需要定期要求委外雲端業者提供相關稽核軌跡進行驗證。

六、雲端服務中斷的緊急應變計畫

委外雲端服務的可用性也是金融服務業需要關注的議題[159]。可用性所指的風險是指委外雲端業者提供服務的可靠度，而這個可靠度包含系統維運的可用性以及儲存資料的可用性兩方面。就系統維運的可用性而言，系統本身所倚賴的軟硬體平台及網路的連通性均是的主要元素，所以是否有足夠的備援機制即是關鍵。備援機制除了可以作用在系統運作時遇到突發的內部事件如軟硬體故障，或是超出預期對系統資源的使用量而導致的影響外，也可以運用在一些外部資安事件如阻斷服務攻擊時，對系統維運可用性所帶來的影響。資料的可用性則是以資料的儲存及備份為主，重視的面相在於資料滅失的風險。

另外一個服務可用性是關於委外雲端業者因為營運問題無法再繼續提供服

[159] Tim Mather, Subra Kumaraswamy, Shahed Latif，胡為君 譯，前揭註 32，頁 70-71 和頁 115-117。參考雲端服務中斷案例包含 2005 年 12 月 Salesforce.com 因為該公司網路節點資料庫故障使客戶無法正常存取資料；2008 年 2 月 AWS S3 服務中斷 2.5 小時；2009 年 5 月 14 日 Google 服務包含 Gmail、Google Docs、Google Calendar 等因路由錯誤而中斷；2020 年 6 月 15 日上午微軟 Azure 於亞太地區發生服務中斷事件，歷時逾 2 小時。2020 年 6 月 10 日上午 IBM 雲發生服務斷線或服務不穩的情況，持續至少 2 小時，且影響範圍遍及全球各地，北美洲、歐洲和亞太地區都有用戶通報無法使用服務。



DOI:10.6814/NCCU202101656

務時，金融機構是否有相關應變計畫完成已雲端化系統的移轉作業，亦即金融機構應就終止或結束委託雲端服務的情況訂定作業移轉計畫，並應於契約終止時，確保受託雲端服務業者全數刪除或銷毀資料，且出具刪除紀錄，作為交易爭議處理依據，也就是所謂的「退場機制」。後續是移轉至金融機構自身建置的環境或是移轉至其他委外雲端業者的環境都需要有具體的實施計畫。這個議題雖然在目前對於提供公有雲服務的主要雲端業者(如 AWS、GCP、Azure 與 IBM)因市場規模與營運策略的發展尚不致發生，但是這仍是金融機構在進行委外雲端服務時無法迴避的議題。

七、資料儲存地點的議題

委外雲端服務中關於資料的儲存地點一直是金融監理機關、金融機構與雲端服務業者三方各有立場的聚焦點。金融監理機關站在保障國家安全、金融市場秩序、監理方便性以及個人資料保護的立場，對於委外雲端業者的客戶資料在地性十分堅持。即便是在 2019 年有條件的進行法規面的調整，但是客戶資料處理地及儲存地，仍以位於我國境內為原則[160]，如需委託境外雲端服務業者，必須符合的要件包括境外當地資料保護法規不得低於我國要求，且金融機構應保有指定資料處理地及儲存地之權力，以利評估境外法律及政治等風險後選擇妥適地點，確保境外雲端服務功能須與境內服務相當，另考量金融機構即時處理業務的便利性及金融監理需要，除經主管機關核准者外，客戶重要資料應在我國留存備份。近來因為 COVID-19 的防疫升級，數家保險公司開始採用視訊投保的方式來進行保險銷售的活動[161]。以往購買保單必須完成與保險業務人員

[160] 請參照「金融機構作業委託他人處理內部作業制度及程序辦法」第 19 之 1 條第 7 項。

[161] Smart 自學網，「疫情期間，有投保需求該怎麼辦？3 分鐘看懂視訊投保、網路投保怎麼做」，2021 年 6 月，https://smart.businessweekly.com.tw/Reading/IndepArticle.aspx?id=6004493 ，最後瀏覽日：2021 年 9 月 1 日。



DOI:10.6814/NCCU202101656

直接見面並且簽名投保的程序，這就是「親晤親簽」的投保規範[162]。但是防疫工作的提升及民眾對於親晤的顧忌，在「親晤親簽」較難執行的狀況下，保險公司被准許以視訊投保的方式來完成投保作業[163]。視訊投保是保險業務員先用視訊錄音錄影等方式確認保戶投保意願後，由保戶簽署要保書、遠距投保聲明書、轉帳/信用卡授權書與電子投保確認書等文件，且錄音錄影讓保險業務員留下紀錄，再將這些文件以拍照或掃描上傳、傳真、e-mail 給保險公司。也可以由業務員先傳要保書 PDF 檔給保戶，保戶以行動載具下載該公司的投保 App 後，用數位簽名回傳給保險公司，然後簽署遠距投保聲明書等其他文件，且用影片錄音錄影，再將這些資料以拍照或掃描的方式回傳給業務員。視訊投保所產生的影音檔案是重要的個人資料，所以當以委外雲端服務作為視訊投保影音檔案的暫時儲存或永久存放的運用時，對於儲存地點必須清楚。

但是，雲端業者的商業模式是求取資源利用的最大化以及成本效益的最佳化，所以在委外雲端服務導入國內的初期，國際級的雲端業者在我國境內都沒有設置儲存資料地點。這也是為何金融機構在委外雲端服務的運用上較其他產業延遲的主因。以目前委外雲端服務的市場來看，業者也逐漸明瞭法令的內容並慎重考慮在國內設置資料中心以存放國內金融機構所委託的服務。即便如此，未來銀行業與保險業在使用委外雲端服務上，如何確認資料的儲存在法規所允許的地點，仍是一個符合監理規範上必須解決的問題。

以上所述，是銀行業與保險業在使用委外雲端服務時所必須要考量到的風險。這些風險有些與前述有關委託雲端服務的一般資訊安全風險具相同性質，

[162] 請參考「保險業務員管理規則」第 15 條相關規定為:「業務員從事前項所稱保險招攬之行為，應取得要保人及被保險人親簽之投保相關文件；業務員招攬涉及人身保險之商品者，應親晤要保人及被保險人。但主管機關另有規定者不在此限。

[163] 請參考「壽險業因應新冠肺炎疫情服務涉親晤親簽與紙本作業之暫行原則」第二條關於親晤親簽暫行措施處理原則，說明視訊錄音錄影方式留存親晤親簽紀錄等相關規定。



DOI:10.6814/NCCU202101656

但也有一些是因為銀行業與保險業的特殊性質及因應該性質所必須遵循的相關法令而產生的特殊風險考量。

## 第二節　委外雲端服務在銀行業與保險業的共同個資議題

一般在探討個資議題時會包含個人資料保護和隱私權保障。個人資料保護是保護個人對自己資料的自主權。自主權的內涵為個人有權決定自己資料是否揭露、在何種範圍揭露、何時可以揭露、以及以何種方式向何人揭露，對於個人資料被他人使用有知悉和控制的權利，對於個人資料也有要求更正或補充的權利[164]。

關於隱私的定義，在不同國家、文化與法律的規範之下會有所不同，而我國憲法中並未明文規定隱私權。[165]。司法院大法官雖在釋字第 293 號解釋中首次出現隱私權之用語[166]，直到釋字第 585 號解釋才承認隱私權是憲法所保障的基本權利[167]，亦即基於人性尊嚴與個人主體性之維護及人格發展之完整，隱私權為不可或缺的基本權利並受到憲法第 22 條保障。其後在釋字第 603 解釋延伸釋字第 585 號解釋的觀點而認為指紋乃個人重要資訊，所以個人對其指紋之自主控制應受到資訊隱私權的保障。釋字第 631 號解釋理由書中則提到我國憲法

---

[164] 范姜真媺，前揭註 5，頁 91-123。貳、個人資料之保護與隱私權之保護; 一、個人資料保護法保護之客體-個資。

[165] 鍾孝宇，巨量資料與隱私權-個人資料保護機制的再思考，國立政治大學法律學研究所碩士論文，頁 41，2017 年 7 月。

[166] 請參考釋字第 293 號解釋文:「...旨在保障銀行之一般客戶財產上之秘密及防止客戶與銀行往來資料之任意公開，以維護人民之隱私權。」

[167] 請參考釋字第 585 號解釋文，對於「三一九槍擊事件真相調查特別委員會條例」中第 8 條第 4 項，認為對個人隱私權保障有欠周延並有違正當法律程序、法律明確性原則應違反憲法意旨。



DOI:10.6814/NCCU202101656

第 12 條規定人民有秘密通訊自由的規定，屬隱私權保障之一種類型，目的是在確保人民在通訊之有無、對象、時間、方式與內容等有不受國家及他人侵擾之權利[168]。

我國實務上對於隱私權認為是屬於不讓他人無端干預個人私領域之權利。具體而言，是指私生活之不欲人知及屬於個人私生活之事務或領域享有自主權且不受不法的干擾，並有免於未經當事人同意的被公開的權利。不過隱私權並非絕對之權利，當隱私與公益相關時，個人的隱私權就會受到限制。綜合而言，隱私權是由維護人性尊嚴及尊重人格權所發展出來的權利，個人能主宰自己私密性的事物，人格才會有價值，隱私權就是在保障人格價值[169]。在釋字 603 號解釋中揭櫫:「惟基於人性尊嚴與個人主體性之維護及人格發展之完整，並為保障個人生活私密領域免於他人侵擾及個人資料之自主控制，隱私權乃為不可或缺之基本權利」，並且，「就個人自主控制個人資料之資訊隱私權而言，乃保障人民決定是否揭露其個人資料、及在何種範圍內、於何時、以何種方式、向何人揭露之決定權，並保障人民對其個人資料之使用有知悉與控制權及資料記載錯誤之更正權」。這些是我國實務上對於隱私權定義的具體說明。

綜合前述可以得知個人資料保護與隱私權保護有部分重疊之處，此部分可稱為「資訊隱私權」[170]。資訊隱私權與一般個人資料都屬個資法的保護範圍內應無疑義。

---

[168] 吳珞齊，保險業適用個人資料保護法問題研究-以保險法第 177 條之 1 及個人資料保護法第 3 條為核心，國立政治大學風險管理與保險學系研究所碩士論文，頁 20-21，2018 年 6 月。

[169] 范姜真媺，前揭註 5，頁 91-123。貳、個人資料之保護與隱私權之保護; 二、隱私權保護之隱私。

[170] 同前註，頁 91-123。貳、個人資料之保護與隱私權之保護; 三、個人資料與隱私。此範圍屬個資法第 6 條所述敏感性特種資料(sensitive information)。



DOI:10.6814/NCCU202101656

在委外雲端服務所需要關注個資保護的議題可以分以下幾個方面:

一、法律合規

委外雲端服務業者都訂有個資保護政策及相關條款而給予使用者相關的保護。而雲端業者所提供的個資保護條款是否適用於當地的法律，尤其在我國是否符合「個人資料保護法」的要求，更甚者如果是金融服務業為使用機構，是否符合主管機關的法規命令或是相關公會所訂的自律規範等，且雲端服務會有跨國界的議題，不同國境內對個資保護的管轄強度與法律亦不相同[171]。

二、資料處理

銀行業與保險業在委外雲端服務中是委託者，也是資料管理者。委託者有權利知道在委外雲端服務中資料是被誰管理及如何被處理。銀行業與保險業可以透過相關的合約規範來要求委外雲端業者提供相關軌跡及紀錄來確認資料是否在所委託的範圍之內進行處理。另外當有需要時，資料管理者也可以隨時要求資料變更。資料擁有者必須能在委外雲端服務的流程中確切掌握到自己所擁有的各類資料分別被以何種方式進行處理，方能掌握隱私權的保障[172]。

三、資料儲存

在委外雲端服務中對於隱私權有極大挑戰的就是關於委託資料儲存作業的議題。以委外雲端服務的作業模式來看，資料的儲存是屬於雲端業者維運及管理事項。在考量資源的有效使用、備援機制與分散風險等因素之下，單一客戶

[171] Tim Mather, Subra Kumaraswamy, Shahed Latif，胡為君 譯，前揭註 32，頁 149。

[172] 同前註，頁 149。



DOI:10.6814/NCCU202101656

的資料儲存地點、儲存方式、備份原則與回復作業等，都是會影響到對個資保護是否周全的程度。在資料儲存地點上由於各國對個資保護的法律控管上強度不一，因此是否可以存放於本國以外的地點就必須考慮，即使可以，當地國的相關法律對於個資的保障是否周全以及當地國對於個資做境外傳輸的規範為何也應納入評估，甚至以委託合約中載明。資料的儲存方式是集中還是分散? 分散式的存放是否位在外國? 有無和其他客戶共用儲存設備? 不同客戶的資料是實體上的儲存設備區隔? 還是邏輯上的系統劃分區隔? 有關資料的備份機制是同地備份還是異地備份? 如果是異地備份，備份資料的存放地點在何處? 這些問題又會回到資料異地儲存上面。在復原機制上，資料的回復地點是在本國? 還是在外國? 如果是在國外，當資料回復後的維運是會將資料駐留在回復地點還是會等原資料存放地恢復可以運作的狀態時再轉回至原資料存放地? 凡是資料所經過或停留的地方就會有個資保護的議題[173]。

四、資料留存和銷毀

委外雲端服務對於資料留存的原則是需要在服務合約中加以載明的。從金融業的監理角度來觀察，委託的銀行業與保險業仍是資料的管理者，需要對於資料有完全的控制權，而雲端業者僅為資料的受託者，應該依照資料管理者的授權和指示進行資料的處理。銀行業與保險業對於交易資料或是個人資料都要依照留存年限的相關規定來執行，所以會與雲端業者透過合約約定來達到相關法令的規範。交易資料會偏重在資料的保全作業，而個人資料除了資料保全之外，當銀行業與保險業收到客戶要求刪除個人資料時，在雲端的個人資料也必須能確認已經完全刪除，因為雲端服務在資料的存儲上可能使用多備份與分散存放的方式，必須能確認被刪除的資料是被完整的刪除才可以符合個人資料保

[173] 同前註，頁 149。



DOI:10.6814/NCCU202101656

護的要求[174]。

五、稽核監測

對於委外雲端服務的使用，銀行業與保險業除了在合約訂立時應該將對於個人資料保護轉化成具體的條文規定放入合約中外，對於實際執行的狀況，也需要透過稽核的作業才能達到監測的目的。在稽核的作法上可以參考業界的遵循標準，再依照業務屬性訂立出稽核內容。所以在個資保護方面的稽核會是以資料流動的過程來判斷是否會有個資遭受到侵害的疑慮或風險。例如，個人資料存放在雲端做資料處理時是否應該只選擇必要項目而非全部都存放；還有像是資料傳輸的中繼點所在國家對於個資保護的控管強度，是否會有資料要被強制監管的疑慮[175]。

六、隱私侵害事件通知與處理

個資受到侵害應當視為資安事件的一種類型，所以在處理上也應該比照相關流程，從發現事件、確認傷害程度、通報相關人員及單位、採取補救措施、檢討疏失與弱點、設定與落實改善方式及定期檢視追蹤。這樣的一套流程持續循環運作是處理資安事件的基本作法。銀行業與保險業在面對資安事件的處理原則並不會因為使用委外雲端服務而有所不同，保護個資的責任還是在資料管理者(亦即銀行業與保險業)的身上，只是還需要和雲端業者訂出清楚的通報作業流程並且確實執行。合約中需要明訂發生個資被侵害時的責任條款。而過失

[174] 同前註，頁 149。

[175] 同前註，頁 150。



DOI:10.6814/NCCU202101656

責任的釐清則需要視個案而定[176]。

銀行業與保險業對於管理資料的個資保護責任並不會因為使用委外雲端服務而移轉至雲端業者。在一般社會通念和法律的認知上，個資安全的義務絕對是由開始蒐集資料的組織或機構承擔，銀行業與保險業不僅是個資的蒐集者，也是使用者及保管者，所以對於個資保護的責任不言而喻。儘管可以透過合約將對於個資保護的責任加諸於雲端業者，但是對於個資保護的最終責任還是不會因為合約關係而被排除[177]。雲端服務的複雜性使得銀行業與保險業對於這種類型服務下的個資保護更不容易確認。這將是需要透過技術和管理不斷強化才能循序解決的議題。

## 第三節　委外雲端服務在保險業營運環節的個資議題

關於保險業運用委外雲端服務所需要討論的個資議題，可以從保險業營運環節的角度來說明。隨著金融科技的日益進步，保險業開始運用保險科技(InsurTech)[178]在營運中，雲端科技的運用也在保險科技的發展項目之中，如前一章所提到的區塊鏈及巨量資料分析等，以下將從保險業的營運面向上使用雲端服務所可能遇到的個資保護問題來說明[179]。

[176] 同前註，頁 150。

[177] 同前註，頁 154。

[178] 李顯正，前揭註 41，頁 15-18。

[179] 李顯正，保險科技如何顛覆傳統保險業的價值鏈？，數位時代，2018 年 3 月，https://www.bnext.com.tw/article/47538/insurtech-value-chain ，最後瀏覽日：2021 年 9 月 1 日。



DOI:10.6814/NCCU202101656

一、銷售與行銷

保險業對於銷售業務與行銷相關的活動採用雲端科技最感到興趣。主要原因在於銷售業務與行銷活動常常需要時效性、方便性與彈性的作業流程支援與相關 IT 技術的配合，所以這方面的運用最為廣泛。目前保險業已經廣泛使用的網路投保平台就是最好的實例[180]。網路投保平台上的行為模式大致上可以區分成確定會成為客戶的保單購買行為(例如意外險或旅平險)以及對產品或相關促銷活動有興趣而在投保平台上進行瀏覽行為的潛在客戶。在進行保單購買的流程中，購買人在保平台上會輸入相關的個人資料，如姓名、身分證字號或護照號碼、居住地址、聯絡電話等，這些屬於個資法中所定義的個人資料。所以一旦購買行為完成，這些資料就會進入投保平台系統後端的資料庫中。

另外一種行為模式是在投保平台上進行保險商品的瀏覽與行銷活動的參與。因為壽險銷售在其產品銷售上有其特定的要求，目前除較簡易的定期壽險可以在網路投保平台直接銷售外，其餘壽險商品多邀約欲購買者在壽險公司的保險平台上留下聯絡資料，例如姓名及連絡電話等，後續再由業務人員以親自聯絡的方式確認該購買者的需求並進行後續服務。準購買者雖然提供的資料較少，但從個資法的角度來觀察，這些資料也是個人資料也會被儲存於保險公司的資料庫中。

保險公司將投保平台由雲端服務的架構例如 SaaS 或是 PaaS 來執行的好處在於雲端服務有較多現成的開發工具及元件可以使用，這些開發工具或套裝元件可以依照保險公司的業務需要進行選用，然後在投保平台上提供新的功能。再透過客戶使用後的回饋意見進行調整，有效率的進行投保平台的功能調整，

[180] 李顯正，前揭註 41，頁 25-27。



DOI:10.6814/NCCU202101656

對於保險公司除了有使用上的彈性[181]，也節省採購流程中所耗費的時間。另外如果是因為行銷活動所產生對網路流量與投保平台網站資源使用量的短期增加也可以做彈性上的調整。典型的 SaaS 應用像是 Salesforce CRM 所提供關於銷售自動化(SFA, Sales Force Automation)[182]、行銷自動化(MA, Marketing Automation)[183]及客戶服務與支援(CSS, Customer Service & Support)[184]整體性銷售及客服的管理。

保險業在這樣的需求下所使用的雲端科技與服務對於個資的問題在於以下幾個層面。首先是客戶資料的儲存問題。無論是購買行為或是行銷行為所留下的個資，在 SaaS 的服務模式下通常是會儲存在雲端的。這樣的儲存一般不會進行資料的加密，因為這樣會使 SaaS 的服務效能在頻繁的資料存取時必須配合反覆加密與解密過程而受到影響，也不符合經濟效益。雲端服務在資料保護上通常著重在防禦來自外部的資安威脅，除了在 IT 科技上使用重量級的解決方案之外，也在各項流程控管上遵循國際標準[185]，像是雲端運算安全聯盟(CSA, Cloud Security Alliance)所發佈的 CSA Guidance 3.0、美國國家科技標準機構(NIST, National Institute of Standards and Technology)所發表公眾雲資安與隱私指引、國標準組織(ISO)發表 27017, 27018 雲端運算資料隱私保護標準(ISO/IEC 27000)、英國標準協會(BSI)所發表個人資料保護(PIMS, Personal Information Management

[181] 同前註，頁 36-40。

[182] Salesforce official website, Salesforce Platform: A Simple Automation Solution for Complex Business Process, https://www.salesforce.com/products/platform/best-practices/business-process-automation/, last visited: 1st Sep 2021.

[183] Salesforce, What is Marketing Automation, https://www.pardot.com/what-is-marketing-automation/, last visited: 1st Sep 2021.

[184] Salesforce, Deliver an unforgettable experience using the world's most complete customer service platform, https://www.salesforce.com/products/service-cloud/platform/, last visited: 1st Sep 2021.

[185] 黃正傑，前揭註 26，頁 14-16。



DOI:10.6814/NCCU202101656

System)機制 (BS 10012:2009 PIMS)等來確保資安管理的完整性與有效性。建立資訊安全管理(ISMS, Information Security Management System)[186]機制除了可以防止來自外部對個資安全的威脅之外，也同時可以做到雲端業者內部的控管。這些機制都是期望能降低個資外洩的風險。

目前已經有 SaaS 服務可以提供資料巨量資料分析服務[187]，但是保險業因為對於將個資透過委外雲端服務來進行巨量資料分析大都還在評估階段，所以目前大多以私有雲的方式來進行。保險業者透過 SaaS 或 PaaS 的網路平台所得到客戶資料，大都會回存於保險業者的私有雲中進行處理，而不會直接在委外雲端的環境執行巨量資料分析。客戶資料中如果是既有客戶群，可以依照購買產品資料分析購買偏好而提供業務單位成交率較高的客戶名單; 如果是潛在客戶群，可以依照需求分析提供產品行銷的目標對象，保險業者利用網路平台所建置的問卷或是瀏覽行為紀錄，都可以成為巨量資料分析的來源，達到精準行銷的商業策略目標[188]。這些資料中屬於業務關係的資料主要是顧客購買保單或留下相關聯絡資訊而可以蒐集到的資料，但是如果是客戶瀏覽網站平台而被辨識出個人的行為紀錄，是否可以與客戶在保險公司所提供的個人資料與購買紀錄等一併進行巨量資料的交叉分析，這屬於個資法上目的外利用與同意權的議題，同時也與個人隱私權的保障有關係，這些議題是保險業要使用雲端科技來進行銷售、行銷或市場調查甚至客戶關懷的營運規劃時必須要考慮的問題。

另外，除了從網路上所獲得的個人資料外，透過電話行銷或是電話銷售所

---

[186] 沈柏村，ISO 27001 資訊安全標準及驗證流程簡介，金融聯合徵信雙月刊，第 10 期，2010 年 2 月， 網址：https://www.jcic.org.tw/main_ch/magazinePage.aspx?uid=215&pid=215，最後瀏覽日：2021 年 9 月 1 日。

[187] 李顯正，前揭註 41，頁 25-27。

[188] 同前註，頁 361。



DOI:10.6814/NCCU202101656

完成的錄音紀錄，現在也有相關的技術可以進行非結構性資料的分析進而成為巨量資料處理的來源之一[189]。因此當所留下的語音內容有包含個資法上所定義的個人資料項目，或是在間接識別上足以判斷出特定個人時，都會被視為個人資料而需要受到個資法的規範。

前述保險業利用各種蒐集資料所進行的巨量資料分析，目前多以私有雲的架構來進行，但是隨著所要處理的資料量增加、資料儲存設備的需求以及分析工具的進步，巨量資料分析會需要委外雲端服務的趨勢也會愈加明顯。綜合而言，保險業者所進行的巨量資料分析，關係到如資料取得是否有經過當事人同意 (如記錄網頁瀏覽的足跡紀錄)、巨量資料的分析是否為目的外利用、資料儲存方式與處理方式的安全性等個資法議題。

二、核保作業

保險核保作業是指保險公司對於投保申請進行審核，進而決定是否接受個案風險而承保，同時也會依照個案的曝險程度計算相關保費的過程。核保作業的過程之中，核保單位對於標的因為承保風險的不同而給遇不同費率的做法，對於保險公司的業務風險性及保證經營的穩定性來說極重要的相關因素，所以業界均視此作業為保險公司的核心業務之一[190]。以人壽保險的核保作業為例，因為人壽保險的保險標的為被保險人的生存與否狀態，考量人的多樣性因素，被保險人除基本的生理因素如年齡和性別外，對於身體健康狀況、個人與家族病史，還有非生理因素如生活習慣及嗜好、居家及工作環境、職業類別等也都

[189] 吳珞齊，前揭註 168，頁 49，2018 年 6 月。

[190] 請參照「保險業招攬及核保理賠辦法」第 7 條第 1 項關於保險業應訂定其內部之核保處理制度及程序，應明訂事項共 13 款，最後瀏覽日：2021 年 9 月 11 日。



DOI:10.6814/NCCU202101656

會納入核保作業的風險評估[191]。以上這些資料的取得，以目前實務上的做法而言，要保人或被保險人必須對於保險標的相關資訊履行據實說明的義務以利保險公司進行核保作業。因為資料多半是由當事人同意的情況之下提供且雙方具有契約關係，所以從個人資料保獲法的角度來觀察應無問題。但是若是從第三方(如醫院)取得與核保相關的個人資料，就必須有資料當事人同意的前提才能蒐集與利用，這是人壽保險公司在進行核保作業時必須要注意到的問題。

核保作業既然是保險業務的核心，核保系統自然也是保險公司核心系統的一環。核保系統的中樞是核保規則的建立與執行，也有稱該部分為核保系統的核保引擎。通常核保引擎會建立在所謂業界最佳範例(Industry Best Practice)的規則，再加上個別保險公司的風險精算模型以及相關法令規定。業界最佳範例與相關法令規定是屬於較為靜態的規則，而風險精算模型則是各家保險公司核保作業的精隨所在。精算模型會依照所輸入的參數資料不斷調整，所以相關基準是較動態的。模型的細緻度與準確度是仰賴巨量資料的處理，所以保險公司能蒐集愈多的資料輸入運算，愈能有精確的風險判斷結果。從使用資料的角度來觀察，最基本的來源是來自於既有保戶的資料，以一般保險所需要提供的個人資料範圍來看，從性別、居住地區、職業、工作場所、個人及家族病史、健康狀況等，均可以成為風險精算模型的參數資料。就個資法的範圍來判斷，使用這些資料來進行核保的處理及利用，應算是目的內的使用。

隨著資訊科技快速的進步，對於核保系統的要求不但要穩定精確，更要能快速反應出結果以便銷售業務的推展[192]。在保險公司還未進行全面資訊化之前，核保作業多半是由銷售端將客戶所提供的投保資料帶回公司內，由建置於公司

[191] 吳珞齊，前揭註 168，頁 50，2018 年 6 月。

[192] 李顯正，前揭註 41，頁 358-359。



DOI:10.6814/NCCU202101656

內部的核心系統處理核保業務。以現今金融科技發展的趨勢來觀察，無論是顧客在保險平台所進行的線上投保或是由保險業務員藉由行動裝置所提供的面對面行動平台投保服務，都希望能達到線上核保的需求，因此這樣的期待勢必在核保系統的架構上要有大幅度的改良，才能達到即時和正確的目標。

然而核保系統因為是在保險公司核心系統的架構之下，能否用委外雲端運算的架構來建置，往往會涉及到保險公司的核心系統是否可以全面委外雲端化的議題。保險核心系統的功能除了核保之外，還有承保、理賠、保單管理、收付費、核賠、再保等系統偕同運作，資料上也是彼此串接，環環相扣。目前無論是線上投保平台或行動投保平台，核心系統多半還是建置於保險公司的內部環境，較先進的方式是在私有雲的架構上構築自行開發及維運的網路投保平台或是行動裝置 APP，再透過電信業者所提供的網際網路服務來完成網路投保或是行動裝置投保的商業目地。因為是私有雲，所以核心系統處理資料的作業都可以視為內部的資料處理，並沒有個人資料處理委外的議題。但是如果將核心系統進行委外的雲端化，首先要考慮的就是個資在雲端服務的儲存地點、儲存方式、查核作業等議題。

另外一種方式，是將核保系統獨立出來使用雲端運算中巨量資料處理的優勢，建立所謂 AI 核保的智慧型模組在委外雲端的平台上，將模組運算結果回送至保險公司的核心系統中提供核保作業所需的結果，僅使用雲端服務的運算能力而不將個資放在雲端。例如將核保系統以 PaaS 的模式建置於雲端服務上，核保引擎(rule engine)的規則與參數設定是資料處理的規則，至於資料的部分則在保險公司內部環境中進行去識別化處理[193]或加密處理，然後再將資料上傳至雲

[193] 劉定基，前揭註 133，頁 53-106。文中說明資料去識別化資料也可以稱為匿名化資料，是指將可以直接識別個人的資料刪除、隱去或是以代碼取代，或將資料以一定條件整合、彙總後以降低個人資料被識別的可能。



DOI:10.6814/NCCU202101656

端的核保系統進行運算，利用雲端運算的資源來完成需要消耗大量 IT 資源的精算模型。但是這樣的方式是需要將資料在雲端將資料做還原或解密後才能處理的，這個部份便會有個資外洩的風險。而且將核保系統功能獨立的做法是否真的符合經濟效益還是需要近一步評估，因為核保系統尚需和其他保險資訊系統進行界接，而獨立在雲端的核保系統對於資料傳輸會增加較多網路資源的耗費且對於系統回應的即時性也是挑戰。

此外，在委外雲端上的核保系統，也可能透過雲端的平台與其他提供資訊服務的公司做業務上的往來，透過與第三方系統界接而取得外部資料而成為精算模型中的參數資料(例如醫療院所、健康存摺等)，然而這些資料應屬於個人資料或是敏感性個人資料，對於這些資料在蒐集時是否取得當事人同意以及資料的處理是否為目的外處理都需要考慮。

三、理賠作業

理賠作業是指當保險契約所載的事故發生時，被保險人備妥相關資料後向保險公司提出申請給付依照保險契約所應支付的賠償金額或是相關責任之金錢給付[194]。保險公司在收到申請文件後會進行相關文件的審核最後做出核賠或是拒賠的決定。在壽險理賠的作業上，被保險人需要提供許多詳實的資料，例如就醫紀錄、病歷資料等，也使理賠作業中使用相關個人資料有適法上的依據。為確保理賠申請的核定正確性，保險公司除了參考申請人所提供的相關資料外，也會參考其他第三方的外部資料。除了壽險公會的同業共享資料之外[195]，其他

[194] 吳珞齊，前揭註 168，頁 51，2018 年 6 月。

[195] 請參照「人身保險業通報作業實施要點」，第 1 條:「中華民國人壽保險商業同業公會（以下簡稱本會）為防止道德危險及危險逆選擇發生，加強各壽險公司間核保及理賠資訊相互交流，並落實通報作業，特訂定本要點。前項通報作業包括收件通報、承保通報及理賠異常件通報三部分。」，另第二條有說明「各壽險公司執行收件通報及承保通報時，應切實依據「保險業通報作業資訊系統操作手冊」每日鍵入通報資料」，是指個公會成員應於每日透過指定的



DOI:10.6814/NCCU202101656

資料的取得如果涉及個人資料的範圍，就必須取得當事人同意。這是進行理賠作業時需要注意的部分。

論及理賠系統，如同前述核保系統一樣該系統也是保險業核心系統的一環，所以大多在建置上會與核心系統緊密結合。隨著金融科技革新所帶動保險科技的進步，在理賠作業上可以運用雲端科技的方向目前有兩個發展，一個是用巨量資料分析所建立的 AI 理賠[196]，另一個是用區塊鏈技術所發展的理賠聯盟鏈。目前已經有保險業者將理賠相關資料進行大數據分析後建立 AI 理賠的模型而應用在理賠服務上，一般案件交由 AI 判讀理賠風險、計算理賠金額，就可直接給付[197]。

AI 要學會審核理賠案件，需先閱讀大量理賠數據，再以機器學習（Machine Learning）中的監督式學習（Supervised Learning）訓練，才能判斷相關資料進而找出每個理賠案件的最佳決策，AI 從讀取理賠資料到完成審核只需要不到 0.5 秒，因此可以大幅提升理賠處理效率，且事後透過大數據驗證 AI 與人工審核結果相似度高達 99.7%[198]。使用系統自動化技術可望大幅提升客戶服務時效，與業界常用的「三日理賠」作為服務效率追蹤指標來相比較，在結合

---

資訊系統向公會通報相關資料。對於新成立保險契約、保險契約異動或是理賠異常表徵的案件均需通報。又參照第 10 條:「本通報資料僅作為各壽險公司核保及理賠時之參考，各壽險公司承保及理賠與否仍應依其實際核保及理賠標準為之。」及第 11 條:「本會及各壽險公司對本通報資料，應建立安全管理機制，除前二條情形外，不得作為其他用途或不當洩漏。各壽險公司核保及理賠人員對本通報資料應依法善盡保守秘密之義務，不得擅自將資料交付或告知第三人，並應切實遵守核保及理賠人員職業道德規範。」指應善盡資料保護及目的內使用。該法規最後更新時間為民國 100 年 6 月 13 日。

[196] 李顯正，前揭註 41，頁 361。

[197] B 型社會企業，AI 保險讓你理賠不再被刁難...估值 20 億美元的「檸檬汁」(Lemonade) 改寫你對風險的定義 更讓每一筆保費有滿滿的社會關懷，019 年 12 月，http://blab.tw/b-media/2019/12/25/ai-20lemonade- ，最後瀏覽日：2021 年 9 月 1 日。

[198] 國泰金控，AI 下圍棋不稀奇 國泰產險推出 AI 理賠服務，資訊中心，https://www.cathayholdings.com/holdings/information-centre/intro/latest-news/detail?news=BdMVl7SEr0OuRoi_LjVXAA ，最後瀏覽日：2021 年 5 月 30 日。



DOI:10.6814/NCCU202101656

金融科技後最快可當天理賠，縮短理賠週期，目的就是給予客戶更快速及優質的服務。但是目前暫時先以傷害險為主，未來將擴大至健康險。有別於產險業的商品型態，壽險業在 AI 理賠上的發展較為緩慢。主要是因為壽險商品的理賠條件較為複雜且理賠資料如病歷、事件紀錄、就醫紀錄等在判讀分析上也需要更多資訊技術的投入，因此需要更長時間建立完整的資料庫並進行大數據分析才會有較好的結果。目前相關的系統發展大多還是以協助理賠人員提升工作效率的輔助角色為主，距離自動化還有一段距離。

除了提升理賠速度，AI 理賠對提高保險公司的風險管控能力也有很大的幫助，以往人工理賠係由理賠人員一件一件地從個案累積審核經驗與準確度，現在 AI 學習全公司所有理賠數據，汲取所有理賠人員經驗值，讓理賠的質與量皆大大提升，多了 AI 理賠把關，能更精準地發掘理賠詐欺案件並即時警示理賠人員異常點，降低理賠詐欺案件的數量[199]。無論是在提升理賠速度或是提高保險公司的風險控管能力，理賠 AI 的發展方式目前大都還是私有雲的架構。主要是因為理賠的相關資料幾乎全部都是個人資料的範圍，所以目前保險業在這部分的發展上在考量法規、監理、資安等因素之下，都還沒有使用委外雲端服務的計畫。

另外一個雲端科技運用則是用區塊鏈技術所發展的理賠聯盟鏈[200]。金管會

[199] AILI，保險業如何透過 AI 革新？我們又如何深陷其中？，https://www.aili.com.tw/message2_detail/56.htm 。該文以英國資料道德與創新中心（Centre for Data Ethics and Innovation, CDEI）於今年九月發佈一份名為《AI and Personal Insurance》的報告，探討 AI 應用可能對保險業造成的改變與其面臨的道德倫理問題摘譯其內容。另參考 GDPR 第 22 條關於個人化之自動決策，包括建檔，該條文 1. 資料主體應有權不受僅基於自動化處理（包括建檔）所做成而對其產生法律效果或類似之重大影響之決策所拘束。衍伸的議題是由 AI 來執行具有法律效果的決策，利害關係人對於決策結果影響自身權益時的救濟手段是否完備。

[200] 陳蕙綾，〈觀察〉11 家保險巨頭組成理賠聯盟鏈 Insurtech 浪潮來襲，鉅亨網，2020 年 5 月，https://news.cnyes.com/news/id/4474678 ，最後瀏覽日：2021 年 9 月 1 日。



DOI:10.6814/NCCU202101656

從 2019 年就要求壽險公會推動保險區塊鏈。區塊鏈就是以網際網路為架構基礎，因為區塊鏈技術有加密性、可靠透明性、不可否認性及不可竄改等特性，因此適合用來解決資料傳輸與信任問題，一旦建置完成，就可以大幅縮短很多作業流程。由壽險公會所規劃的保險區塊鏈，包括「電子保單、保單存摺、理賠與保全」四大功能，以處理大量的保單通報資訊的角色發展[201]。其中，電子保單在 2019 年已完成相關試辦工作，陸續由新光人壽、國泰人壽、富邦人壽、台灣人壽與南山人壽等壽險公司，試辦日額醫療通報功能，當保戶向其中一家申請理賠，只須交一份醫療證明，另外四家有承保同一保戶日額醫療險的壽險公司，都會接到通報，同步理賠，保戶可省去每一家都申請理賠的工作，且理賠速度也會加速，大約 1～3 天就可全數撥款。同時，利用區塊鏈，醫院可以用數位化加密資料來傳遞相關保戶病歷與住院資料，加速保險公司確認醫療過程與判別理賠金額，達到即時理賠的效果，讓保險服務更貼近消費者需求。金管會於 2020 年更進一步同意 11 家保險公司組成命名為「保全／理賠聯盟鏈」的保險區塊鏈聯盟，於當年 7 月 1 日起可試辦透過區塊鏈，讓保單要保人可辦理線上資料變更，及受益人可在線上辦理健康險與傷害險的醫療理賠。

這個聯盟區塊鏈的架構基本上是由壽險公會所建置保全/理賠雲為中心，相關參與的保險業者共同加入這個聯盟鏈之中，而聯盟中對於資料交換的格式、對接程式的語言、檔案傳輸所用的通訊協定及加密協定等均有統一的規範和技術規格，這樣才能在資料交換的效率及防護上有完整的解決方案[202]。理賠作業

[201] 請參考「中華民國人壽保險商業同業公會辦理電子保單存證作業規範」。第 2 條:「本會辦理電子保單存證作業，應遵守保險法、洗錢防制法、個人資料保護法、電子簽章法、金融消費者保護法、保險業作業委託他人處理應注意事項、其他保險相關法令及自律規範之規定。」，依照該規範，中華民國人壽保險商業同業公會為電子保單資料的保管者，受公會會員之委託保存電子保單相關交易存證資料。

[202] 請參考「保險業辦理「保全／理賠聯盟鏈」業務應遵循事項規範」。第 7 條:「...（五）資料傳輸與資訊安全...2.壽險公會共享平台留存資料傳輸與接收紀錄，保險公司得隨時透過區塊鏈技術檢視紀錄與傳送狀態。...」，壽險公會為共享平台的管理者，負責提供資料交換服務並提供適當的安全措施，公會僅保留資料交易紀錄，也無對保單資料進行處理或利用的行為。以



DOI:10.6814/NCCU202101656

所處理的資料多為個人資料的範疇，而採用參與者與限制性的聯盟區塊鏈可以因讀取和寫入規格、加解密技術、資料處理速度等方面的標準化好處，視為較妥適的模式[203]。以目前理賠聯盟鏈的運作的方式，主要是以簡化理賠程序為目的去執行跨聯盟成員間資料處理與交換，雲端平台是由壽險公會負責建置，壽險公會負責該平台的技術規格、資料格式等標準制訂。但需要注意的是壽險公會的平台也是建置於中華電信的機房中，這應該算是一種 IaaS 的委外服務。

四、保全作業

保險的保全作業是指為了使保單能夠按照客戶投保時約定的情況持續有效，最根本的就是要讓客戶有持續需要保險或持續滿足的感覺。保險公司為了滿足客戶不斷變化的需求，維持契約的持續有效，就必須提供各種服務，也就是通常所說的售後服務，一般保險的售後服務稱為契約保全。保險保全在作業上主要包括保險契約的關係人變更、基本資料變更、復效、掛失補發、保單遷移、保險金額的增加或者減少、退保、保費墊交、減額交清、保單紅利退發、滿期給付等服務項目。一般而言，保單資料的變更屬於契約的變更因此必須審慎處理。有屬於影響範圍較小如通訊地址、聯絡電話等，也有影響層面較大者如要保人的變動、受益人的變動或是保險金額之調整等。但是無論是大或是小，這些都是個人資料的變動。保全作業的良好與否是關係到保險公司對客戶服務的品質以及其他與保單相關作業結果的正確性。從保險公司的資料流來看，保全作業是屬於資料處理上游的階段，自然對於下游各作業或相關系統有著重要的

個資法的角度來看，定位上應接近於資料的處理者。

[203] BINANCE-ACADEMY，私有鏈、公有鏈和聯盟鏈有何區別？，2021 年 4 月，https://academy.binance.com/zt/articles/private-public-and-consortium-blockchains-whats-the-difference#consortium-blockchains，說明聯盟區塊鏈聯盟鏈是「將少數同等權力的參與方視為驗證者，而不是像公有鏈那樣開放的系統，讓任何人都可以驗證區塊，也不是像私有鏈那樣，通過一個封閉的系統，只允許某一個實體來任命區塊的生產者。」，最後瀏覽日：2021 年 9 月 1 日。



DOI:10.6814/NCCU202101656

影響。

目前保險業在保全作業上的雲端科技運用應屬 2020 年 7 月由金管會同意試辦的「保全／理賠聯盟鏈」[204]。這個聯盟鏈的形成與架構與前述的理賠聯盟鏈是相同的系統架構與技術規格，只是所處理的事務屬於保全方面的業務。而且為了要做到保戶單一申請、文件共通，這 11 家參與試辦的保險業者，已經把線上理賠申請書、契約變更申請書等欄位與格式統一，讓彼此的文件可共通。這樣便可以透過區塊鏈技術，讓保單要保人可辦理線上資料變更。這些先行加入聯盟的保險公司包括新光人壽、國泰人壽、台灣人壽、南山人壽、富邦人壽、元大人壽、中國人壽、全球人壽、第一金人壽、國泰產險及富邦產險。凡是上述加入聯盟鏈公司的保戶，例如國泰人壽保單的要保人要變更保單地址，但這位要保人同時也是富邦人壽、新光人壽的保戶，只要改國壽的保單資料，就會通過「保全聯盟鏈」，直接完成所有其他保單的地址變更，保戶不用再逐一與相關的保險公司進行保單變更。保險區塊鏈的發展有助以更迅速便捷的方式服務保戶，除此之外，保險局將進一步推動電子保單認證與存證機制，鼓勵保險業推動電子保單，且存放在第三方認證機構，在消費者對電子保單的真偽有所爭議時，得由公正第三方提供保單內容，確保保單的保障範圍。

如同理賠聯盟鏈，保全聯盟鏈所面對的個資議題是相同的。因為保全聯盟鏈的業務與保險契約的內容變動有關，大部分為與個人資料有關的變動。聯盟鏈的概念基本上算是封閉式的，也就是只開放給特定的成員使用，且成員的權限都有依照對象進行不同的設定，所以這樣的形態是取用區塊鏈的優勢如加密技術與可以追溯傳送紀錄和狀態的透明性，但是並不採用去中心化的概念。主要在於由壽險公會所負責的共享平台為區塊鏈資料傳輸的維運，將各加入聯盟

[204] 李靜宜，前揭註 70。



DOI:10.6814/NCCU202101656

鏈的會員有共享資料的利益。平台雖只是 IaaS 的服務模式，但是仍需注意資料暫存的問題以及因為加密技術所產生金鑰保管的議題，。

保險業雖然是金融業的一環，但是因為其業務特殊性所以在委外雲端的運用上與其他金融行業(如銀行)相比仍有不同之處，本節針對保險業在運用委外雲端服務上所需面對的個資議題加以說明。從以上的論述不難看出委外雲端的個資議題始終與資料存儲的位置有著密切的關係。資料在哪裡，資安議題就在哪裡。在 IaaS 的模式上，資料會在委外雲端廠商的必要性比較低，大都可以由保險機構自行存儲資料，所以在個資安全問題上需要評估的因素就比較單純; 但是在 PaaS 或是 SaaS 的模式上，因為技術面和效率面上的考量，導致資料在委外雲端廠商的必要性是高的，所以個資安全問題上需要評估的因素就比較多元與複雜。針對保險業幾個主要的業務流程如銷售行銷、核保、理賠、保全等在雲端科技上的運用分別從個資安全的角度加以檢視，算是在面對保險科技(Insurtech)日新月異的同時，應該也需要重視這些科技所帶來的個資議題。

保險業在委外雲端服務上需要討論的議題就是關於資料跨國境傳輸的部分。我國個資法對於跨國境的傳輸是採「原則允許，例外禁止」的態度。相較於歐盟 GDPR 的相關規範是採「原則禁止，例外允許」的出發點來看，我國是採較寬的原則[205]。保險業在金管會的監督管理及同業公會相關的自律規範之下，一直都是在個人資料必須在地化的原則，國際傳輸或境外存放資料幾乎是不可行的。雖然在 2019 年 7 月後開始對於金融業使用委外雲端服務有條件的放寬這樣的原則，但是目前保險業普遍還是以儲存資料在地化的可行性作為評估業務雲端化的首要條件。這部分在第二項關於銀行業與保險業委外雲端服務的資安議

[205] 劉定基，前揭註 133，頁 66-69。



DOI:10.6814/NCCU202101656

題中已經說明。

保險業在使用巨量資料分析的目的是要達到以 AI 來輔助營運，例如精準行銷、智能核保、智能理賠等。AI 的核心技術是機器學習與深度學習[206]。機器學習是電腦根據大量數據分析後歸納出規則或建立演算法模式。深度學習也是針對特定領域的大量資料使用演算法計算出最佳結果，並且演算法可以透過演算結果的累積來提升後續演算準確性，有自我學習的效果。但是機器學習或深度學習在資料蒐集的廣度與深度，資料整理方法的準確性等都會影響基礎資料的偏誤程度，而分析資料的規則或建立模式的客觀性，也會影響 AI 結果而引發可能有歧視性的議題，這些都是運用 AI 時要考慮的。因此若運用 AI 所產生的結果有影響個人權益或是有歧視性的決策時，應當要有法律介入及人為補救的機制。目前因為實務上 AI 運用的範圍僅為輔助的角色或試驗階段，所以該議題尚未被重視，但這將是一個隨 AI 運用日趨多元而必須面對的議題。

[206] 李顯正，前揭註 41，頁 346 - 347。



DOI:10.6814/NCCU202101656

# 第四章　我國銀行業與保險業委外雲端服務規範與個人資料保護

本章將對於我國銀行業與保險業在委外雲端服務上應適用的相關規範進行說明。從「個人資料保護法」(以下簡稱「個資法」)的角度來分析委外雲端服務時，銀行業與保險業是委託人也是資料管理者，而委外雲端服務業者是受託人也是資料處理者。在這樣的關係之下需要說明的法規包含「個資法」、「個人資料保護法施行細則」(以下簡稱「個資法施行細則」)、「金融機構作業委託他人處理內部作業制度及程序辦法」(以下簡稱「委外辦法」)、「保險業作業委託他人處理應注意事項」(以下簡稱「委外注意事項」)、「保險業辦理資訊安全防護自律規範」(以下簡稱「自律規範」)及「金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法」(以下簡稱「維護辦法」)。這些法規對於委外雲端服務的運用都有直接或間接的影響。使用委外雲端服務要符合相關法規並達到個人資料保護的目標，就需要以合約來完成。因此本章也將以實例說明委外雲端服務合約的架構與內容。最後會將相關法規與合約實例進行對比分析以供參考。

## 第一節　委外雲端服務的相關規範與個人資料保護

我國金融業對於雲端服務及相關科技一直都保持關注的態度，但是因為金融監理機關對於雲端服務的運用在開始時是以較保守的態度來回應，所以金融業在雲端服務的使用上大都僅在與個人資料較無關係的領域來進行，像是利用社群媒體進行行銷廣告，或是利用雲端服務與跨業合作進行市場問卷調查來蒐集非個人資料的客群喜好，用來開發新產品或是擬定品牌市場策略。由於資訊科技的持續更新使網路化及行動通訊成為主流，在此趨勢之下帶動五大數位化



DOI:10.6814/NCCU202101656

的發展，包括物聯網(Internet of Things)、社群(Social Network)、行動(Mobile)、數據分析(Analytics)、雲端(Cloud)[207]。這些發展改變人們的消費行為、生活模式、產業型態與社會發展。進而顛覆傳統商業的經營模式，使行銷策略快速改變，因而也使金融產業受到衝擊。從 Brett King 在「Bank 3.0：銀行轉型未來式」[208]書中所提出「銀行不再是一個地方，而是一種行為(Banking is no longer a place you go, but something you do.)」的觀點，可以說明金融服務將可以透過科技跳脫時間與空間的侷限，而採取更主動、更直接的方式貼近客戶。金管會順應此一趨勢，開始於 2014 年規劃「打造數位化金融環境 3.0」之政策[209]，並在兼顧風險與科技趨勢的前提下，開始逐漸鬆綁法規，鼓勵金融業掌握經濟與社會結構變遷脈動，創新商品、服務及經營模式。

2019 年金管會對於金融業在雲端科技的使用上有了大幅度的政策調整，從原本沒有明文禁止但卻不鼓勵的曖昧態度，轉變成在特定條件之下可以允許金融業使用雲端服務的具體政策。為了讓金融機構能適當運用雲端科技，同時能兼顧消費者權益保護，金管會參考了各國對金融機構作業委託雲端業者處理應該遵循的規範，決定以循序漸進開放原則，修正「委外辦法」部分條文。金管會釋出的修正條文中提到，金融機構作業委外，如果涉及客戶資訊，應於契約簽訂時訂定告知客戶的條款，未訂有告知條款的金融機構，得書面通知客戶委外事項，並依「個資法」規定辦理[210]。而金融機構將作業委託他人處理，涉及

[207] Bong De Ungria, SMACIT: Social, Mobile, Analytics, Cloud, Internet of Things, TransFORMe, Feb 2016, https://bongdeungria.com/smacit-social-mobile-analytics-cloud-internet-of-things/, last visited: 1st Sep 2021.

[208] 盧韻雅、何翠婷，《Bank 3.0》及《Digital Bank》帶動金融創新，財金資訊股份有限公司，https://www.fisc.com.tw/Upload/c8992963-eb29-4d6a-b760-59e0425372c6/TC/8302.pdf，最後瀏覽日：2021 年 9 月 1 日。

[209] 金融監督管理委員會，打造數位化金融環境 3.0 全面啟動，https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=201501130003&toolsflag=Y&dtable=News，最後瀏覽日：2021 年 9 月 1 日。

[210] 李靜宜，銀行資料上雲端，金管會准了！符合條件境外公雲也能用，iThome，2019 年 6 月，



DOI:10.6814/NCCU202101656

使用雲端服務時，要遵循委外辦法中的相關規定。

此外，金管會將依照雲端作業委外是否具重大性，區分為「核准制」以及「備查制」[211]。具有重大性的委外作業，或是要將作業委託到境外的金融業者，都須採取申請核准制，事先向金管會提出申請。若不是屬於此範圍的委外作業，則是採取備查制。以下則為銀行業及保險業有關委外雲端服務的相關辦法及規範。

### 第一項 個人資料保護法與個人資料保護法施行細則

「個資法」與「個資法施行細則」中雖然對於委外雲端服務沒有直接的法律規定，但是仍可以從雲端服務中儲存的資料是否為個人資料及雲端服務者的法律地位與責任來討論。

在雲端服務中的資料可能會經過去識別化、加密或切分等方式處理，經這樣處理後的資料是否屬於個資法的保護範圍需要先加以說明。依「個資法」第2條第1款的規定「得以直接或間接方式識別該個人之資料」均視為個人資料的定義來看，雲端服務環境中的資料在傳輸或儲存的過程雖然以前述的處理方式而無法直接識別特定個人，但是若有方式可以間接識別特定個人，該資料仍應屬個人資料的保護範圍。如同「個資法施行細則」第 3 條補充說明關於不能直接識別的資料，只要透過和其他資料對照、組合、連結等方式後而足以識別該特定個人，就仍然是在個資法的適用範圍內[212]。就銀行業與保險業使用委外雲端服務的情境而言，雖然相關資料在傳輸或儲存時可能經過去識別化、加密或

---

https://www.ithome.com.tw/news/131515 ，最後瀏覽日：2021 年 5 月 31 日。

[211] 同前註。

[212] 劉定基，前揭註 133，頁 69-70。



DOI:10.6814/NCCU202101656

切分等方式處理而不具直接識別性，但因銀行業與保險業本身即保有可供對照組合的原始資料、加解密金鑰及存取權限，因此對其而言，相關資料屬於個人資料而有個資法的適用，應無疑義。

至於雲端服務業者在個資法上的法律地位為何，需要先判斷其是委託機關還是受託機關。這部分在「個資法」第 2 條中並無明確定義，但是從「個資法施行細則」第 8 條中委託機關對受託機關的監督事項中，可以得知委託機關與受託機關的區別，在於委託機關有權決定個人資料蒐集、處理或利用的範圍、類別、目的與期間，受託機關僅能在委託機關預設的範圍內，實際進行資料的蒐集、處理或利用[213]。將委託機關和 GDPR 中所規定「資料管理者」相比較，可以得知兩者之間對於資料都有權決定使用方式和目的，受託機關或 GDPR 中所定義的「處理者」則是為資料管理者蒐集、處理或利用個人資料[214]。

將上述資料管理者和受託者的區別標準用在銀行業與保險業使用外雲端服務的模式上，銀行業與保險業應視為資料管理者或是委託機關，屬於「個資法」上的權責主體，雲端服務提供者是處理者或受託機關[215]。在這樣的關係之下，依「個資法施行細則」第 8 條[216]及第 12 條[217]規定，銀行業與保險必須對於所委託的雲端業者進行適當的監督，而監督的事項也有必須涵蓋的範圍；再依「個資法」第 4 條[218]及「個資法施行細則」第 7 條[219]規定，雲端業者所提供的服務

[213] 同前註，頁 78。

[214] 同前註，頁 79。

[215] 同前註，頁 80。

[216] 個資法施行細則第 8 條參照。

[217] 個資法施行細則第 12 條參照。

[218] 個資法第 4 條參照。

[219] 個資法施行細則第 7 條參照。



DOI:10.6814/NCCU202101656

也當受個資法的（間接）規範。

## 第二項 金融機構作業委託他人處理內部作業相關辦法

### 一、金融機構作業委託他人處理內部作業制度及程序辦法

委外辦法是依據2006年9月18日行政院金融監督管理委員會金管銀（五）字第 09500386200 號令訂定發布後開始實施。在2019年9月30日完成最近一次的修正，而委外雲端服務正是修正重點。誠如立法總說明所提及修正的目的是讓金融機構在使用委外雲端服務上有明確的法律規定，也希望金融機構在運用委外雲端服務改善金融作業時，對於風險評估、資料安全、緊急應變等面向需審慎考量，以維持對金融機構服務的品質與對客戶權益的保障。本次修法最須關注之處乃新增之第19條之1、第19條之2相關條文。雲端服務的內容與運作層面具有多樣性且複雜度高，既有的第19條僅針對金融業將作業項目委託至「境外處理」做相關規範，因此並不能滿足在委外雲端服務這樣作業模式的監督和管理需求。新增之條文給予金融業在使用委外雲端服務上的明確法源依據，補強第19條的不足之處。以下即針對上述兩條加以分析。

委外辦法第19條之1規定:「金融機構將作業委託他人處理涉及使用雲端服務，應依下列規定辦理」。該敘述開宗明義指出金融機構只要是將委外作業以雲端服務的方式來處理時，就必須符合此條文內容的規定。

第 1 款規定:「金融機構應確保作業風險控管，充分評估受託機構處理之風險，採取適當風險管控措施，確保作業委外處理之品質，並應注意作業委託雲端服務業者之適度分散。」此規定之立法理由是考量雲端科技是高度整合性的資訊技術，其服務的深度與廣度會因為金融機構所要委託的業務範圍而有所不同。因此當金融機構要使用委外雲端服務時，除了對於廠商的服務在品質上透



DOI:10.6814/NCCU202101656

過服務水準協定(SLA, Service Level Agreement)予以具體化確保之外，也要完整的評估資訊安全以及個人資料保護的相關風險。一般對於雲端服務提供廠商所做的資安能力評估，大多會檢視廠商是否有資訊安全的相關認證，這是關於資格的部分，另外對於廠商所提供的技術性解決方案，也會從資訊安全科技的角度來衡量，這樣才能做到較完整的風險評估，採取適當的風險管制措施。另外金融機構對於委託雲端服務業者的業務範疇，必須要納入企業資訊治理 (IT Governance)[220]的長期規劃中，以避免因為過度集中於單一雲端服務業者而產生服務中斷的風險。

第 2 款規定:「金融機構對雲端服務業者負有最終監督義務，並應具有專業技術及資源監督雲端服務業者執行受託作業，並得視需要委託專業第三人以輔助其監督作業。」此規定對委外雲端服務的責任歸屬明確加以規定之。該規定可以看出主管機關對於委外雲端業者與金融機構在雲端服務的關係中將金融機構定位成委託機構而委外雲端業者是受託機構。在這樣的架構之下來觀察個資法的適用時，金融機構應被視為資料的管理者，是個人資料保護的責任主體。委外雲端業者因為是資料的處理者或受託機關，需遵照委託者所指定的範圍來處理個人資料，雖然不是個人資料保護上的責任主體，但是會以與委託者訂立契約的方式承擔一定的法律義務和責任[221]。需要注意的是，主管機關的目的應該是要金融機構即便透過與委外雲端業者的契約關係，也不能轉嫁或減少其對於個人資料保護的責任，從金融監理的角度來看，是一個明確的問責(accountability)方式[222]，可以有效率的處理因使用委外雲端服務所產生的個資保

[220] Gartner，IT Governance (ITG), https://www.gartner.com/en/information-technology/glossary/it-governance, last visited: 1st Sep 2021.

[221] 劉定基，前揭註 133，頁 80-84。

[222] Tim Mather, Subra Kumaraswamy, Shahed Latif，胡為君 譯，前揭註 32，頁 154。



DOI:10.6814/NCCU202101656

護或是其他相關問題。另外關於監督的部分，因為考量到雲端服務的多元性與技術的複雜度，所以准許金融機構可以委託專業第三方輔助監督作業[223]。關於「專業」應該需綜合評價第三方的相關證照資格及業界經驗為依據。而第三方也僅為「輔助其監督作業」，並不具有相關監督責任。

第 3 款規定:「金融機構應確保其本身、主管機關及中央銀行，或其指定之人能取得雲端服務業者執行受託作業之相關資訊，包括客戶資訊及相關系統之查核報告，及實地查核權力。」本款的立法意旨在於金融業的委外業務需視為金融機構自身業務的延伸，所以應該以自身受監督的相同標準來檢視。金融機構的主管機關為金管會，但是委外雲端業者的主管機關可能為經濟部。因此委外雲端業者在個人資料保護的強度與做法與受高度監理的金融機構有所不同此一要求就是在處理不同行業別之間跨業合作時所應遵循的標準，亦規定金融機構、主管機關及中央銀行或其指定之人對受託作業具取得資料及實地查核權力[224]。這是行政管轄權的聲明，因為委外雲端業者目前大都為跨國級企業，因此若委外雲端服務涉及境外委託時，金融機構應依本辦法第 18 條第 1 項及第 2 項規定[225]，取得受託機構所在地金融主管機關同意主管機關查核之書面文件，或由受託機構出具同意主管機關查核之同意函。但是本項規定關於主管機關及中央銀行執行境外實地查核的部分則尚無實例可以參考。

第 4 款規定:「金融機構得自行委託，或與委託同一雲端服務業者之其他金

---

[223] 顏志仲，金融業資料上雲鬆綁 細說監管作為與技術考量，網管人，2020 年 10 月，https://www.netadmin.com.tw/netadmin/zh-tw/viewpoint/959D89FBB3B848E7AE56678D88C60960 ，最後瀏覽日：2021 年 9 月 1 日。

[224] 李靜宜，銀行資料上雲端哪些新規定？實地查核怎麼做？金管會雲端委外 8 大重點一次看，iThome，2019 年 7 月，https://www.ithome.com.tw/news/131678 ，最後瀏覽日：2021 年 9 月 1 日。

[225] 請參照「金融機構作業委託他人處理內部作業制度及程序辦法」第 18 條。



DOI:10.6814/NCCU202101656

融機構聯合委託具資訊專業之獨立第三人查核，並應符合下列規定：(一) 確認其查核範圍涵蓋雲端服務業者受託處理作業相關之重要系統及控制環節。(二) 應評估第三人之適格性，以及其所出具查核報告內容之妥適性並符合相關國際資訊安全標準。(三) 應針對金融機構所委託作業範圍進行查核並出具報告。」此規定指當金融機構對於所委託之雲端業者進行查核時，可以採自行或與其他使用同一雲端業者的金融機構聯合委託具資訊專業之獨立第三人進行查核。對於查核結果的要求標準，乃以本規定之第一目到第三目為原則。因此，第三方進行查核時即使是採聯合委託的方式，仍須針對個別金融機構所委託雲端服務的範圍提出相關查核報告，不可以一般性通則報告替代。同時，委外雲端業者也不行以自身所取得之相關國際標準認證來替代第三方查核報告。本規定意在提供非單一方式的查核選項以及明定查核報告所應具備的基本條件。

第 5 款規定:「金融機構傳輸及儲存客戶資料至雲端服務業者，應採行客戶資料加密或代碼化等有效保護措施，並應訂定妥適之加密金鑰管理機制。」這項規定最值得注意的是關於資料加密的要求。從法條文意觀察，當金融機構使用委外雲端服務時，在資料傳輸上已經不能只做到傳輸方式的加密而已，必須更進一步要做到資料的加密才能進行傳輸的作業。而儲存在雲端業者的資料更是需要進行加密機制的處理。除了資料加密之外，將資料進行去識別化也是一種保護資料的方式。有加密機制，就會有金鑰管理的議題。本規定明示金鑰管理機制必須建立，至於管理方式則由金融機構與雲端服務業者共同協議為之。這樣規定所造成的影響在第三章第一節第二項中有相關的說明。如金鑰產生的方式與保管的方式都必須納入管理機制中。

第 6 款規定:「對委託雲端服務業者處理之資料應保有完整所有權，除執行受託作業外，金融機構應確保雲端服務業者不得有存取客戶資料之權限，並不得為委託範圍以外之利用。」本規定再次重申金融機構與委外雲端業者屬委託



DOI:10.6814/NCCU202101656

者與受託者的關係，所以雲端業者居於受託者的角色僅能在委託者所在指示範圍內對資料的蒐集、處理及利用。金融機構是委託人，同時也是資料管理者與法律上的責任主體，所以應透過契約方式與雲端業者協議出具體受託業務並限制雲端服務業者進行受託範圍以外的資料利用。同時資料存取權限的控管應該由金融機構來掌握。值得注意的是在委外雲端環境中，雲端業者還是擁有最高權限的系統管理者，因此金融機構要能確保雲端業者的資料存取權限以及沒有做委託範圍以外的資料利用，必須檢視或稽核相關軌跡或紀錄以達到確保的目的，金融機構可以要求雲端業者提供具不可竄改性的軌跡，例如將軌跡資料以自動化方式即時同步提供金融機構。

第 7 款規定:「委託雲端服務業者處理之客戶資料及其儲存地以位於我國境內為原則，如位於境外，應依下列規定辦理：(一）金融機構須保有其指定資料處理及儲存地之權力。(二）境外當地資料保護法規不得低於我國要求。(三）除經主管機關核准者外，客戶重要資料應在我國留存備份。」此規定目的為確保金融監理權有效行使，及迅速有效處理客戶爭議，故金融機構委託雲端處理之客戶資料及其儲存地以位於我國境內為原則。客戶資料處理地及儲存地如位於境外，境外當地資料保護法規應不得低於我國要求，且金融機構應保有指定資料處理地及儲存地之權力，以利評估境外法律及政治等風險後選擇妥適地點，確保境外雲端服務功能可與境內服務相當。此外，考量金融機構即時處理業務之便利性及金融監理之需要，除經主管機關核准者外，客戶重要資料應在我國留存備份，這部分的要求也與資料的保全有關。至於客戶重要資料則是指關於客戶存款、授信、信用卡、匯款及投資等資料(第 3 條參照)。

本規定除了從金融監理的角度來考量外，對於個人資料保護也有其意涵。在委外雲端服務上要做到個資保障，資料管理者必須能明確掌握資料的儲存狀態與處理方式，例如儲存於何處、以何種方式儲存、保障措施為何、以及儲存



DOI:10.6814/NCCU202101656

當地對於個人資料保護和隱私權的法律規範強度為何等。主管機關訂立規定的目的應是要求金融機構在選擇委外雲端服務時應把資料安全性確保的條件為前提考慮，該規定實質上會與本條文第 3 款金融機構應確保其本身、主管機關及中央銀行實地查核權力及第 6 款的對委託雲端服務業者處理之資料應保有完整所有權，共同建立起金管會對於委外雲端服務使用的基本管理方向。

第 8 款規定:「金融機構應訂定妥適之緊急應變計畫，降低因作業委託而可能有服務中斷之風險。金融機構終止或結束作業委託，應確保能順利移轉至另一雲端服務業者或移回自行處理，並確保原受託雲端服務業者留存資料全數刪除或銷毀，並留存刪除或銷毀之紀錄。」從國際標準的資訊安全管理目標來衡量，資訊安全的管理目標是要做到資料的機密性(Confidentiality)、完整性(Integrity)、可用性(Availability)的完善，降低資訊安全的意外風險[226]。本規定的目的就是針對可用性的部分加以明定之。除了為確保金融機構不因雲端服務業者發生無法處理受委託作業，導致中斷客戶服務情事，故金融機構應訂定妥適之緊急應變計畫外，金融機構亦應就終止或結束委託之情況訂定作業移轉計畫，並應於契約終止時，確保受託機構全數刪除或銷毀資料，要求雲端服務業者出具刪除紀錄並予以留存，作為交易爭議處理依據。本規定要求金融機構必須預先備妥委外雲端服務的退場機制計畫才算完整。

委外辦法第 19 條之 2 也是關於委外雲端服務所新增的條文。當金融機構欲使用委外雲端服務的業務具重大性或是依同法第 18 條會將作業委託至境外時，必須檢具相關書件向主管機關申請核准始得辦理。相關書件於規定於第 19 條第 1 項第 1 款至第 5 款，包括依該法第 4 條第 2 項訂定之委外內部作業規範[227]、董

[226] 沈柏村，前揭註 186。

[227] 請參照「金融機構作業委託他人處理內部作業制度及程序辦法」第 4 條。



DOI:10.6814/NCCU202101656

(理)事會決議之議事紀錄或外國銀行在台分行之總行授權人員出具同意書、法規遵循聲明書、作業委託雲端服務業者處理之必要性及適法性分析其中應包括對雲端服務業者遵守我國客戶資料保護相關規定之評估、委外作業計畫書等。委作業計畫書應包含: 風險評估及管理機制、資訊安全及管理、客戶資訊及相關系統之查核報告及確保實地查核權力之說明、緊急應變計畫及退場機制。

本條也明定重大性作業的認定條件，並依照重大性與否將委外雲端服務區分為「核准制」以及「備查制」。具重大性作業的委外或是將作業委託到境外的情況，都需先向金管會申請核准[228]。而非屬於此範圍的委外作業，則是採取備查制。外國銀行在台分行及在台子銀行作業委託總行、母行或所屬集團之分支機構及子公司，複委託雲端服務業者處理，應檢具該條第 1 項作業委外計畫書併同第 18 條規定書件向主管機關申請核准[229]，相關辦理規定亦在條文中載明。

二、保險業作業委託他人處理應注意事項

「保險業作業委託他人處理應注意事項」(以下稱「委外注意事項」)於行政院金管會 99 年 7 月 21 日金管保理字第 09902558341 號令訂定並開始實施，而最近一次修正為金管會 108 年 12 月 26 日金管保壽字第 10804958391 號令修正，主要也是針對保險業使用委外雲端科技的相關規範。從整體架構和條文內容來觀察，新修正的內容是將「委外辦法」進一步細緻修改為適用於保險業的相關辦法，因此二者在目的性與功能性上並無太大差異。其中對於保險業使用委外雲端科技的相關注意事項分別列於第 17 之 1 點及第 17 之 2 點。上述條文的架構

[228] 請參照「金融機構作業委託他人處理內部作業制度及程序辦法」第 19 條之 2。該條文中所稱具重大性之作業，係指下列情形之一：「一、受託作業如無法提供服務或有資訊安全疑慮，對金融機構之業務營運有重大影響者。二、受託作業涉及客戶資料安全事件，對金融機構或客戶權益有重大影響者。三、其他對金融機構或客戶權益有重大影響者。」

[229] 同前註。



DOI:10.6814/NCCU202101656

與「委外辦法」中的第 19 條之 1 及第 19 條之 2 相似。

在「委外注意事項」中需要在委外雲端服務中一併考量的是第 16 點及第 17 點所規定的事項。第 16 點是有關於委託至境外的業務向主管機關申請的規定，此點與「委外辦法」的第 18 條規範結構大致相同。此外，第 17 點是關於保險業將作業項目委託至境外處裡所需遵從的相關規定。此點亦與「委外辦法」的第 19 條的規範結構相同。因此不再多做說明。

### 第三項 金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法

「金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法」(以下稱「安全維護辦法」)於 2013 年 11 月 8 日公布實施，全文共計 16 條，分別於 2015 年 7 月及 2016 年 5 月各修正一次。該辦法為金管會依據個資法第 27 條第 3 項[230]授權所訂定，金融業在擬定企業資訊安全政策及執行資訊安全管理時的重要依據。金融業在面對主管機關的資訊安全及個人資料保護業務的監理查核或是企業進行內部及外部的資訊安全稽核時，也多會以該辦法為合規的基準。

而該辦法的架構除總則之外，還包括個人資料保護之規劃、個人資料之管理程序及措施、個人資料之安全稽核與紀錄保存及持續改善機制，與「個資法」第 6 條關於特種個人資料的保護、第 7 條關於書面同意的規定、第 19 條關於非公務機關處理個人資料之要件、第 20 條關於非公務機關利用個人資料進行目的外利用的情形、第 11 條關於個人資料更正或補充及權責等相互援引，所以「安

[230] 個資法§27III: 前項計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關定之。



DOI:10.6814/NCCU202101656

全維護辦法」其實就是金融業的「個資法」的具體規定。

因此，當金融業在進行委外雲端服務的規劃時，執行方向會是以「委外辦法」的第 19 條之 1 為基本原則，再輔以「安全維護辦法」為執行方法的各個面向而逐一展開，並以此與委外雲端業者在契約上、服務水準協定上及工作說明書(SOW, Statement of Work)上建立完整規範的合作關係。

### 第四項 保險業辦理資訊安全防護自律規範

依「保險法」第 165 之 1 條保險業需成立同業公會並須加入公會始能經營保險事業。再依同法第 165 之 2 條第 1 項 1 款:「訂定共同性業務規章、自律規範及各項實務作業規定，並報請主管機關備查後供會員遵循」，此為同業公會訂定自律規範的依據。中華民國人壽保險商業同業公會(以下稱「壽險公會」) 所訂立的自律規範是我國保險業內稽內控監理法制架構中重要組成元素。依照「保險業內稽內控實施辦法」第 6 條第 1 項規定，保險業使用電腦化資訊系統處理者，其內部控制制度，除資訊部門與使用者部門應明確劃分權責外，至少應包括該條文所列的十四項控制作業，並依所屬商業同業公會訂定自律規範辦理，且定期檢討資訊安全自律規範[231]。據此壽險公會訂定「壽險業辦理資訊安全防護自律規範」。

「自律規範」原名稱為「壽險業辦理資訊安全防護自律規範」。於 2013 年 12 月 26 日金融監督管理委員會金管保綜字第 10200145480 號函准予備查訂定發布全文 12 條。最近一次修正為 2020 年 5 月 26 日金融監督管理委員會金管保綜字第 1090419516 號函准備查，修正發布名稱及全文 16 條。如同自律規範第 1 條

[231] 趙偉傑，前揭註 6，第三款 商業同業公會自律規範，頁 136-137。



DOI:10.6814/NCCU202101656

所述:「中華民國人壽保險商業同業公會與中華民國產物保險商業同業公會為督促會員公司資訊業務與相關資訊資產之安全，發揚自律精神，防範資訊處理作業過程發生影響資訊及系統機密性、完整性及可用性之安全事件，確保各會員公司資訊處理作業能安全有效地運作，特訂定本自律規範。」

在自律規範中，有關於雲端服務的規定包括，第 2 條關於雲端服務的定義:「雲端服務：係指服務提供者以租借方式提供個人或企業得承租其網路、伺服器、儲存空間、基礎設施、資安設備、系統軟體、應用程式、分析與計算等資源，以達資源共享之服務。」此定義應已涵蓋第二章所有委外雲端服務的類型。而第 8 條則提到:「各會員公司若有運用新興科技（包含雲端服務、社群媒體、生物特徵資料及自攜裝置等），需依據保險業運用新興科技作業原則（如附件三）辦理，以建立完善之控管機制，降低新興科技之運用風險。」[232]

在現行法制運作下，保險業的內控內稽機制，為個別保險業經國家授權，在一定框架內(保險業內控內稽實施辦法)所自訂之內部管理規範，呈現出國家借重私規範(內控內稽機制)來填補、具體化法律制度(保險監理法制)之規範制定公私協力現象[233]。近年來保險業監理的執行方向顯示個別保險業經國家授權所訂之內控內稽機制，並不只是維持私規範身分來與保險監理法律制度合作，已經被轉介成為具有法律性質的裁罰構成要件，成為行政法可以適用之法。個別保險業所形塑之內部管理規範體系，透過保險法第 171 條之 1 第 4 項規定之立法轉介，就規範位階而言已如同保險法，就法效性而言也同樣取得保險法之法效性[234]。從以上可以看出「自律規範」中關於委外雲端服務的規範也是保險業必

[232] 關於保險業運用新興科技作業原則所述與委外雲端服務相關的安全控管規範共計 11 條，這些項目與「金融機構作業委託他人處理內部作業制度及程序辦法」第 19 條之 1 相互配合。

[233] 趙偉傑，前揭註 6，第一款 借重保險業內部管理規範，頁 146。

[234] 同前註，第二款 直接授權轉變為間接授權，頁 148。



DOI:10.6814/NCCU202101656

須遵守的法規之一。

目前銀行業與保險業在使用委外雲端服務時所需要遵守的規範包括「個資法」、「個資法施行細則」、「委外辦法」、「委外注意事項」、「自律規範」及「維護辦法」。綜合前項說明後有以下的評論:

「個資法」目前對於委託機構和受託機構仍無明確的定義，委託機構和受託機構各自所代表的權利主體與應該負擔的責任需要在個資法中明定，未來在委外雲端服務的運用上對於這部分的確認十分重要。目前實務上委託機構和受託機構之間以合約中連帶責任的條款將主管機關對於委託者所需要承擔個資法的罰則延伸至受託者。

雲端服務廠商可以提供即時的監控儀表板功能，除了對委託機構提供即時的資源使用資訊外，也可以提供資料分佈的儲存地點與儲存量的即時資訊、系統使用帳號即時列表等，使委託機構有更同步、便利的監督方式，對於「委外辦法」的合規性有加強的效果。

在國外的機房是否可以進行主管機關的實地查核，參考目前處理國際貿易公平競爭與反托拉斯的事件經驗，從資料蒐集的角度來看待主管機關對於查核權力的行使，透過資料的完整性與透明性可以協助監理作業的執行。所以在境外執行實地查核，對於當地行政機關的管轄權並不會有不良的影響，也可以達到監理互助的目標。

雲端服務廠商可以主動提供聯合委託的稽核模式，與第三方查核機構合作，提供委托機構可以共同查核的機制。這種模式對委託機構和雲端業者均可以節省投入稽核作業的資源並增加稽核效率，若進一步透過合約形成制度化的執行模式，對主管機關的監理作業也可以成為標準化的依據。



DOI:10.6814/NCCU202101656

委外雲端業者在資料處理或儲存地點都會面臨資料主體所適用法律與資料儲存或處理當地法律重疊適用的議題，實務上對於資料儲存地的法律與我國「個資法」比較後，業者多以較嚴格的法律為遵守標準。「委外辦法」中規定雲端業者處理或儲存資料地點以我國境內為原則，該項規定與雲端服務的特性相衝突，恐將造成雲端服務運用上的限制或是跨境服務的貿易障礙。是否應對資料處理或儲存地點做限制可視資料的性質而定，例如用個人資料與非個人資料的區分或用資料機密等級來決定可否至境外處理，這是該項規定可以改善的部分。

關於異地備援或是相關備援機制不應只考慮資料的部分，對於備援機制的網路容量能力及系統服務的關聯性應該一起納入，以避免 single point failure 的狀況發生。該項規定除要求有妥適的緊急應變計畫外，應該增加定期演練的規定，以確認備援機制的可執行性，才能達到該項規定的目的。

金管會對於委外雲端服務在境外地點的資料保護法規程度、金融機構所需檢具的書審資料及與國際間個資保護法律上的接軌，可以考慮從 DPIA (Data Protection Impact Assessment)[235]的方向建立較為具體化的監理框架，將目前條文中所規定較為模糊的部分如國外法規保護程度的高低比較及需要檢具的書審資料內容等，建立具體的標準以增加法規的可執行性。

目前的法律規範大都偏重在對於雲端服務使用的合規性上，但是對於運用雲端服務後所產生的科技成果則缺乏相關法律。例如智能合約是否以現今民法就足以處理關於程式自動履約行為，又如區塊鏈的加密機制被破壞後所產生的

[235] 請參照 UK GDPR Articles 35 (1) and 35 (7), https://www.legislation.gov.uk/eur/2016/679/article/35 。



DOI:10.6814/NCCU202101656

法律問題等，較妥適的方式應該訂立特別法來處理對此類科技成果的法律議題。

關於 AI 也是相同的議題。目前我國對於 AI 並沒有專屬的法律進行規範，而 AI 的法律議題有兩個方向需要探討，第一是建立 AI 的方式，第二是 AI 的運用。AI 建立的方式是需要透過大量資料的蒐集、處理和利用，有些資料的蒐集目的和因應 AI 需要而處理與利用的目的未必契合，這種屬用目的外利用的行為當然應依照「個資法」來處理，但是目前實務上發展 AI 的機構並沒有針對這部分進行合規性的檢視，這是需要改進的地方。再者，對於使用網站行為的軌跡資料是否可以蒐集，目前「個資法」中並無明確規範，在網路活動與網路科技蓬勃發展的趨勢下，「個資法」應該對於這樣的行為增訂相關法律以避免隱私權遭受侵害。

另一方面是關於 AI 的運用。我國目前對於 AI 用途尚無相關的法律規範，關於 AI 用途的立法可借鏡歐盟於 2021 年 4 月所提出的「人工智慧規則(AI Act)草案」[236]對於 AI 系統以風險程度分為不可接受風險、高風險、有限的風險及最小的風險四類，其中不可接受風險是禁止 AI 的使用; 如社會評分或公共場所生物辨識執法，而高風險類的 AI 使用會受到嚴格的控管; 如信用評分、教育考試的評分、招聘流程等，該草案目的是防止 AI 的運用會產生個人隱私權侵害及歧視性決策，而形成對人格權保障的疏漏。這方面的法律立法應該在 AI 尚未廣泛運用前先做準備。

[236] 請參照 European Commission，Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence，https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1682 ，最後瀏覽日：2021 年 10 月 15 日。



DOI:10.6814/NCCU202101656

## 第五項 委外雲端合約應注意事項

有別於一般消費者個人使用，企業在選擇委外雲端服務時須考量多面向的問題。當企業評估是否雲端化時，所面對的問題就是既有的內部資訊系統移轉至雲端平台或是直接採用雲端服務的選擇。考慮的著眼點包含採用混合式雲端服務牽涉到既有應用系統或軟體與雲端服務的技術整合外，委外雲端服務在跨供應鏈服務商之間服務水準、資訊安全與個資保護的責任關聯性等，在各種營運資料經過多層服務商不同層面的作業後，有關資料保護的疑慮，都是影響決策的主要因素，同時也必須將雲端服務提供者與使用者間的權利和義務用合約化的方式呈現。

大多數的使用者在與雲端服務業者簽訂契約時多為定型化契約[237]，這樣架構下的契約對於價格、服務水準、資訊安全及隱私權的保障多半是維持既定的條款不會調整。當雲端業者調整服務或是系統時，其通常可以單方面的進行變更而不需要考慮對使用者可能發生的影響，所以一般說來這樣的變動會是使用者不可控制的風險。使用者對於自己資料的儲存地點也無法明確知道，更不可能清楚資料儲存國家的公務單位是否有權獲取特定用戶的資料以及和自己國家的相關法規有無抵觸等。企業在作雲端服務採購時，合約內容除了應重視委外雲端服務有關的應用系統導入及維運的作業技術的整合外，也應對軟硬體架構及網路環境等技術相關條件作詳細敘述。此外對於智慧財產權所歸屬、保密條款、資訊安全與隱私權保障、合約終止、違約罰則等權益保護的條款，也必須仔細審酌[238]。

---

[237] 請參見「消費者保護法」第 2 條。

[238] 中華人民共和國香港特別行政區政府，採購雲端服務的實務指南，https://www.infocloud.gov.hk/home/10791?lang=tc ，最後瀏覽日：2021 年 5 月 31 日。



DOI:10.6814/NCCU202101656

對於透過採購雲服務來達成部分業務營運目標的企業而言，在決定購買何種雲服務及向哪家雲服務商購買之前，不論是否只能接受定型化契約，都應該先就以下的事項進行風險評估，即使接受定型化契約的條文，也可將風險限縮在可承受的範圍；若能直接與雲服務商談判合約內容，則更可保障自身利益。

一、委外雲端服務提供者與簽約主體

國際雲端大型廠商在我國所進行的委外雲端業務，是直接由原廠簽訂合約，或是由原廠授權之代理商為簽約對象，因涉及合約關係究竟存在何主體之間是需要確認的，以及與該合約對何者可以主張相關權利與負擔責任是有著直接關係[239]。直接與原廠建立合約關係比較單純，若是以原廠授權之代理商為簽約對象時，應確認合約中所議定的條款對於原廠究竟發生如何效力，原廠的責任義務為何，就需要明訂於合約中。當發生法律問題需要以法律程序解決時，合約所適用的準據法與爭端解決方式及訴訟地點也需要在合約中確立。

二、委外雲端服務合約之性質

當雲端業者有部分服務項目是屬於外包性質時，與客戶簽訂的合約條款是否有記載於該雲端服務商與外包商的合約中，以確保該外包商可履行對最終用戶的合約義務。而當雲端服務商要更換外包商時，是否需要通知使用者並取得其同意，或是使用者有權力可以因此而中止契約，這些也需

[239] 樂以媛，如何用合約替雲服務採購把關，政府機關資訊通報第 336 期，2015 年 10 月，頁 4。



DOI:10.6814/NCCU202101656

要在合約中載明[240]。

三、委外雲端服務之服務內容與服務水準協議

合約服務內容主要的部份就是指服務範圍的說明。包含服務運作、服務的承諾與保證、服務水準三大重要項目。服務運作中包含所採用的維運原則、維運程序與技術以及監控方式。同時也應以業界最佳作業(Best Practice)模式為基準設定有關品質管理、資訊技術服務管理及安全管理等具體化指標作為檢視的依據。服務的承諾與保證是要在合約中確保雲端廠商的陳述和使用者的要求相符合並且條文化，這部分需要注意雲端廠商在合約中所註明關於免責聲明、責任限制、免責條款，是否與相關法令相牴觸而有效力上的問題。服務水準是合約協議的重心之一。依照前述維運服務的指標可以設定出具體的服務水準。服務水準須清楚界定服務達成的期望目標並具有與所提供的服務有相關性及充分性，客觀且合理的衡量方式，並且說明未達服務水準時所需要採取的對應行為。使用者應有足夠的權限可以對合約中所同意的服務水準進行查核[241]。

四、委外雲端服務之資料處理與保護

關於資料處理與保護的部分，委外雲端的合約中需要約定的事項包含委託者可以限制其實體資料存放地點以符合我國金融業的監理要求。委託者對於所擁有的資料有完全的控制權力，可以不受限制的存取資料並且可以要求受託者遵照委託者的需求方式儲存及管理資料，對於受託者使用及處理個人資料的方式也應清楚界定於合約中，這包含了關於個人資料的修

[240] 同前註。

[241] 中華人民共和國香港特別行政區政府，前揭註 238，頁 33-38。



DOI:10.6814/NCCU202101656

正、刪除或凍結等相關資料變更原則及程序。合約應載明受託者於合約期間不可以隨意變更資料相關服務的約定(如資料的儲存方式與地點、備份方式等)，而當可能影響個人資料處理之服務因特殊理由欲調整時，須得到委託者的同意與確認後才能變動。受託者對於資料保護的程序和做法是依照何種技術性或是組織性的標準，以及在個人資料保護上的所遵循的法律均應記載於合約條款中[242]。

五、資料所有權歸屬

委外雲端服務的合約中應對於資料所有權應以條款確認之。有關資料所有權的部分，需對於在雲端所儲存或建立的資料明定為資料管理者或委託人所有，雲端業者對於提供服務所產生的營運資料，例如系統軌跡紀錄、資料存取紀錄等，則為資料的擁有者，但應在合約中以明文約定在特定條件之下雲端業者須配合提供。

六、費用計價相關說明

雲端服務費用的計價方式與價格需在合約中明定。使用者在採購前對於所採用的服務內容在使用費率上應做業界比較，關於費用計算的明細項目也應在合約中說明，例如收費的計量單位 (資料傳輸是以檔案大小或是封包)、是以資源分配量計費還是資源使用量計費等，有無最短服務合約期間的限制，或是最低使用量的限制，當提前終止合約時的賠償條件及資料轉出時的相關費用。當使用者需要增加或減少服務的質(如服務項目)與量(如

[242] 樂以媛，前揭註 239，頁 4-5。



DOI:10.6814/NCCU202101656

使用硬體資源)時，其計費方式的說明[243]。

七、遷入與遷離雲端服務

任何委外的服務都需要考慮到採用、移轉和停用的議題，委外雲端服務亦是如此。合約生效日期與服務啟用日期在特定狀況下並不一定相同，尤其是對於資料儲存地點或方式有客製化的需求時更會以專案方式處理。在委外雲端服務需要移轉至其他雲端服務供應商或是終止服務需要移回委託者端時也需要有對應的處理方式。考量合約的性質，委外雲端服務的遷入、移轉和停用遷出應該在合約中以一般性的條款說明，而用工作說明書為合約附件，詳述該部分合約雙方的職責及執行方式等，這樣架構對於合約的完整性較為周全[244]。

八、違約處理與罰則

服務的違約主要會來自於雲端廠商對於所承諾的服務目標或應交付的結果無法達成所致，所以合約中對於雲端廠商所承諾的目標必須清楚且可以具體化衡量，這樣才可以在必要時啟動違約條件的確認及相對應的罰則。違約罰則一般來說會因合約價值而有其上限並且可以將其上限訂於合約中。另外一種違約是關於可歸責於雲端業者的過失所導致委託者在民事或刑事上的司法判決賠償及行政機關裁罰的結果，例如「個資法」的損害賠償或罰則可能有鉅額的賠償金額。這部分就不應在合約中用賠償上限的條款加以限制。因此，雲端服務使用者在雲端業者違約時可以使用的權利，像是

[243] 中華人民共和國香港特別行政區政府，前揭註 238，頁 21-22。

[244] 同前註。



DOI:10.6814/NCCU202101656

合約終止權、損害賠償、違約金等都應在合約中保留之[245]。

綜合上述，金融業在委外雲端服務的合約注意事項因為其服務的複雜性及相關法規的規範，所以須注意的面向繁多，必須謹慎為之。雖然資訊安全與個人資料保護的部分為關注的重點，但是在採用委外雲端服務時需要納入合約中的條件也不僅限於這部分。其中像是服務水準協定的衡量指標、廠商的維運能力評估、跨國法律的合規性、資料中心管理成熟度等都須納入選商及合約的考慮項目中，方可避免日後爭議與降低風險。

### 第六項 小結

「個資法」是我國對於個人資料在蒐集、處理及利用為避免人格權受到侵害，並促進個人資料之合理利用而實行的法律，是規範個人資料保護的基礎法律，屬於普通法的性質[246]。而金融業為實現該法律要求所衍伸出相關辦法或規範就包含前述「委外辦法」、「維護辦法」、具法律法效性的「自律規範」及「委外注意事項」。金融業因為有其產業上的特性而受到高度監管，所以當執行面上有所需要時，也會有要配合的特別法規。以金管會有條件放寬金融業使用委外雲端服務的政策為例，所對應的相關辦法是較為嚴格的。例如「委外辦法」第19條之1第7款，就直接以確保監理權之有效行使及迅速處理客戶爭議為考量，要求委外雲端服務之處理與儲存客戶資料地點應以我國境內為原則，境外處理為例外。綜合言之，保險業欲使用委外雲端服務時，法規面的考量除了「個資法」和「個資法施行細則」外，主管機關所公佈之相關規定或辦法，以及同業公會所訂立且報備主管機關函准的自律規範等，都是需要一併納入考量的。此

[245] 同前註，頁 42-48。

[246] 林洲富，個人資料保護法之理論與實務，原照出版公司，2019 年 10 月，頁 3。



DOI:10.6814/NCCU202101656

外，關於委外雲端服務的合約應注意事項的內容，除了服務內容與服務品質的載明外，也應將相關法規所需遵守的事項納入合約條款中。

## 第二節　委外雲端服務合約實例說明

### 第一項 IBM 雲端服務合約說明

本項以 IBM 的委外雲端合約為說明範例。IBM 的雲端委外服務合約稱為「雲端服務合約 Cloud Service Agreement (CSA)[247]」，其性質相當於委外雲端服務的主合約，規範合約雙方之權利和義務，「雲端服務合約」再加上「交易文件(Transition Documents; TD)[248]」或是「附件(Attachment)[249]」就會成為完整的 IBM 委外雲端服務合約。「交易文件」是詳細記載委外雲端服務內容的文件，性質與工作說明書(SOW)類似。「雲端服務合約」的架構分成:雲端服務、內容及資料保護、「雲端服務」之變更與停售、保證、收費稅捐及付款、責任與賠償、合約期間與終止、準據法及適用地區及通則。以下就「雲端服務合約」中與個資保護和委外服務關係相關要點說明:

一、雲端服務

1. IBM 的雲端服務為透過網路所提供的即時性服務，例如 SaaS、

[247] 請參照 IBM，雲端服務合約 Cloud Service Agreement (CSA)，https://www.ibm.com/support/customer/csol/terms/#detail-document，相關說明為:「完整合約」:本「雲端服務合約(CSA)」及適用之「附件」與「交易文件(Transaction Document; TD)」為構成本「雲端服務合約」相關交易之完整合約，貴客戶得依「本合約」約定訂購「雲端服務」。

[248] 請參照 IBM，「交易文件 Transaction Documents: Transaction Documents (TDs) 」說明:「交易文件」規範交易之具體詳細內容，例如：計費及「雲端服務」之說明與相關資訊。「交易文件」包括工作說明書、服務說明、訂購文件及發票。可能有多個交易文件適用於單一交易。

[249] 請參照 IBM，「附件 Attachments」: 指明為「附件」之「文件」，訂有若干交易類型（例如：解決方案附件）共同適用之補充條款。



DOI:10.6814/NCCU202101656

PaaS 和 IaaS，服務的內容都會載明於「交易文件」 中。IBM 雲端服務基本上都是全年無休，如有因為維護時間而會有服務受到影響的狀況時會預先通知使用者。有關技術支援及服務水準也會載明於「交易文件」或是「附件」中[250]。

2. 有關非 IBM 所提供之服務，指 IBM 得提供第三人「雲端服務」，或者，「IBM 雲端服務」得啟用對第三人「雲端服務」(「非 IBM 服務」) 之存取權限。「交易文件」載明所適用之第三人合約條款，據以規範客戶對「非 IBM 服務」之使用。對「非 IBM 服務」之使用，視同客戶同意前揭第三人合約條款。IBM 非前揭第三人合約條款之當事人，對於「非 IBM 服務」不負任何責任。[251]。

3. 客戶訂購、登記、使用「雲端服務」或支付其款項，即視為客戶接受「雲端服務」適用之「附件」或「交易文件」。IBM 確認訂單或啟用存取權限時，即接受貴客戶之訂購[252]。

4. IBM 將提供為供應「IBM 雲端服務」所需之設施、人員、設備、軟體及其他資源[253]。「啟用軟體」係指客戶下載至客戶系統，用於協助使用「雲端服務」之軟體，該軟體將載明於「交易文件」[254]。客戶應提供為存取及使用「雲端服務」所需之硬體、軟體及網路

---

[250] IBM，雲端服務合約，https://www.ibm.com/support/customer/csol/terms/#detail-document ， 1. 雲端服務, a. IBM 雲端服務。

[251] 同前註 ，1. 雲端服務, b. 非 IBM 服務。

[252] 同前註，1. 雲端服務, c. 訂單之接受。

[253] 同前註，1. 雲端服務, d. IBM 所提供之項目 。

[254] 同前註，1. 雲端服務, e. 啟用軟體。



DOI:10.6814/NCCU202101656

連線，包括所需之貴客戶特定 URL 位址及相關憑證等[255]。

5. 客戶之授權使用者僅得於客戶所取得授權之範圍存取「雲端服務」[256]。任何使用者以貴客戶之帳號認證使用「雲端服務」，該等使用者之行為均由貴客戶負責。

二、內容及資料保護

1. 「內容」包含客戶或其授權之使用者所提供、授權存取或輸入於「IBM 雲端服務」之所有資料、軟體及資訊。客戶授與 IBM、其關係企業及其等之承包商行使下列行為之權利與權限：為提供「IBM 雲端服務」而使用、提供、儲存及以其他方式處理「內容」。使用 IBM 雲端服務並不會影響客戶對於所提供內容的擁有權或授權[257]。

2. 關於內容的使用，IBM 公司、其關係企業及其等之各別承包商僅得以提供及管理「IBM 雲端服務」之目的存取及使用「內容」。IBM 同意除 IBM 員工及承包商因交付「雲端服務」所必要者外，不得將「內容」揭露予他人[258]。

3. 客戶應負責取得一切必要之權利與權限，及授與該等權利與權限，於「IBM 雲端服務」中處理「內容」。客戶為於「IBM 雲端服務」

[255] 同前註，1. 雲端服務, f. 貴客戶所提供之項目。

[256] 同前註，1. 雲端服務, g. 使用權及貴客戶責任。

[257] 同前註，2. 內容及資料保護, a. 貴客戶所提供之「內容」。

[258] 同前註，2. 內容及資料保護, b.「內容」之使用。



DOI:10.6814/NCCU202101656

中處理個人資料（包括個人資料或其他受規範之資料），而提供、授權存取或輸入該等資料前，應依法律之規定為揭露並取得同意。倘若有任何「內容」可能受政府管制或所要求之安全措施可能超出 IBM 就「IBM 雲端服務」所訂定之安全措施，除非適用之「交易文件」中特別明文許可，或 IBM 事先以書面同意執行額外之安全和其他措施，否則客戶不得提供、准予存取或輸入內容」於「IBM 雲端服務」中處理[259]。

4. 「IBM 資料安全與隱私權政策」(IBM Data Security and Privacy Principles (DSP)) 適用於正式發佈之標準「IBM 雲端服務」。「IBM 雲端服務」之特定安全特定功能(feature) 與其他功能，均規範於適用之「附件」或「交易文件」。客戶應負責選取、訂購、啟用及使用適用於支援客戶使用本「雲端服務」之可用資料保護特定功能(feature)。客戶應負責評估「雲端服務」在貴客戶預期用途上及「內容」上之適用性。客戶同意所使用之「雲端服務」係符合貴客戶之需求及關於法律遵循所需之處理指示[260]。

5. 「IBM 資料處理附錄」(DPA)其中載明 IBM 處理貴客戶資料之方式。若有適用 i) 歐洲一般資料保護規章(EU/2016/679) 或 ii) http://www.ibm.com/dpa/dpl 所載明之其他資料保護法之情形，則於其適用的範圍內，「內容」所含個人資料適用前揭 DPA 及所適用之「DPA 附件」。於當事人之一方提出要求時，IBM、客戶或其等各別關係企業應照規定格式，就「內容」所包含之受規範個人資料

[259] 同前註，2. 內容及資料保護, c. 貴客戶責任。

[260] 同前註，2. 內容及資料保護, d. 資料保護。



DOI:10.6814/NCCU202101656

依法訂立附約。雙方同意（並將確保其各別關係企業同意）前揭附加合約應受「本合約」條款之拘束[261]。

6. 就具有自行管理特定功能之「IBM 雲端服務」，客戶得隨時移除「內容」。否則，本公司將於「IBM 雲端服務」期滿或終止時，或基於貴客戶之要求，歸還或移除 IBM 運算資源中之「內容」。本公司不保存「內容」，但若干「內容」可能留存在「IBM 雲端服務」備份檔中，直到該等檔案依 IBM 備份保留實務規範期滿為止[262]。

三、「雲端服務」之變更與停售

IBM 基於提供特定功能、改善對於服務的承諾、配合現行採用之作業與安全標準或適用法律等情況下，有權對於改變雲端服務的內容[263]。IBM 會協助客戶在服務期間內將已經撤回的服務項目移轉至 IBM 其他服務上。對於非 IBM 的服務，IBM 或是第三方協力廠商可以於任何時間不再提供其服務[264]。

四、保證

IBM 的保證將針對 IBM 的雲端服務在「交易文件」中所描述的使用做合理的保障及技術提供。保證會隨著雲端服務終止而一併結束。IBM 所提供的保證具有全部擔保責任的性質，會取代其他保證[265]。IBM 的保證具有

[261] 同前註，2. 內容及資料保護, e. IBM 資料處理附錄。

[262] 同前註，2. 內容及資料保護, f.「內容」之移除。

[263] 同前註，3.「雲端服務」之變更及停售, a. IBM 變更「雲端服務」之權利。

[264] 同前註，3.「雲端服務」之變更及停售, b. 雲端服務之停售。

[265] 同前註，4. 保證, a. IBM 保證。



DOI:10.6814/NCCU202101656

以下的限制[266]:不保證 IBM 的雲端服務會服務不中斷或是無錯誤的維運。不保證所有的問題都會修復。不保證可以預防所有來自第三方的破壞或是未經授權的存取。不適用於當問題來自於非 IBM 所造成的誤用、修改、損壞，或未遵守 IBM 的書面文件所造成的失敗。IBM 對於試用服務或非 IBM 的服務只會提供現況同意書，沒有任何保證服務。第三方合作廠商可能會提供非 IBM 的服務提供保證。

五、責任與賠償

1. IBM 所負擔的所有責任的請求金額都以合約所記載的內容為準。無論請求基礎為何，就因「本合約」所生及與「本合約」相關之全部請求，IBM 所負之全部責任，以客戶所受之直接實際損害為限，且賠償金額以客戶就造成損害之個別服務所支付之款項為賠償上限。IBM 對於特殊損害、附帶損害、懲罰性賠償、間接損害、衍生之經濟損害，或所失利益、商業機會、價值減損、營收、商譽或預期節省之成本不負賠償責任。這些限制對於 IBM 及其聯盟商、合約商及供應商有集體性的效用[267]。

2. 第三方的求償若是因為客戶的資料、設計、其他因客戶運用所產生的求償，亦與 IBM 無關[268]。

六、合約期間與終止

[266] 同前註，4. 保證, a. 保證之限制。

[267] 同前註，6. 責任與賠償, a. 損害賠償責任限制。

[268] 同前註，6. 責任與賠償, d. 責任限制。



DOI:10.6814/NCCU202101656

有關期間的開始，是以 IBM 通知客戶「雲端服務」可以開始使用為起始日。「交易文件」中會載明雲端服務是否為自動續約，續用的相關基準，以及何時為服務中止日[269]。當客戶有重大違約或違反安全、法律、客戶義務、及使用者條款的情況發生時，IBM 得暫停提供雲端服務。對此，IBM 將會於停止客戶使用雲端服務前對客戶發出通知。若是暫時停止服務的原因是可以補正的，IBM 將會通知客戶所必須採取的恢復行動，若是客戶無配合執行，IBM 將會終止雲端服務[270]。客戶可以在以下三種狀況對 IBM 雲端服務提出 30 日後終止的通知:「若在適用之法令修訂或「雲端服務」變更後，政府或主管機關提出書面建議時」、「若「IBM 雲端服務」之變更致客戶無法遵循適用法律者」、「若 IBM 通知客戶，將進行對客戶使用「雲端服務」有重大不利影響之變更時」。客戶依據以上的情況所提出的終止要求，對於雲端服務中非 IBM 的服務也具有相同的適用[271]。

七、準據法及適用地區

任一方應各自負責遵循下列規定:「適用於其業務與『內容』之法令規章」、「進出口及經濟制裁法令規章」[272]。關於法律的適用要點中主要為[273]:

1. 雙方同意適用台灣之法律為準據法，但不適用該準據法之法律衝突原則。

[269] 同前註，7. 合約期間與終止, a.「雲端服務」之期間。

[270] 同前註，7. 合約期間與終止, b.「IBM 雲端服務」之暫停。

[271] 同前註，7. 合約期間與終止, c. 雲端服務之終止。

[272] 同前註，8. 準據法及適用地區, a. 法律遵循。

[273] 同前註，8. 準據法及適用地區, b. 適用法律。



DOI:10.6814/NCCU202101656

2. 任一方之權利及義務僅於客戶公司地址所在國家有效。

3. 倘若貴客戶或任何使用者出口或進口「內容」，或在台灣領域以外地區使用「雲端服務」之任何部分，則 IBM 不作為該項目之輸出者或輸入者，但資料保護法令另有規定者不在此限。

4. 「本合約」若有任何條款被認定為不生效力或無法強制執行者，其餘條款仍具完整效力。

5. 「本合約」對於不得以合約免除或限制之消費者法定權益不生影響。

八、通則

1. IBM 為獨立承包商，與貴客戶間未成立代理、合資、合夥或信託等關係。IBM 不承擔貴客戶履行任何法定義務之責任，亦不就貴客戶之業務或營運承擔任何責任，貴客戶對其「雲端服務」之使用應自負其責。IBM 僅作為資訊技術提供者[274]。

2. 本合約之其他一切變更均須由雙方以書面接受始生效力[275]。

3. IBM、其關係企業，以及其等之承包商，需要使用業務聯絡資訊與若干帳戶使用資訊。前揭資訊非屬「內容」。帳戶使用資訊為啟用、提供、管理、支援、實施及改善「雲端服務」所需之資訊。帳戶使用資訊範例包括利用追蹤技術（例如：使用「IBM 雲端服

[274] 同前註，9. 通則, a. IBM 之契約地位。

[275] 同前註，9. 通則, b. 雲端服務合約之變更。



DOI:10.6814/NCCU202101656

務」期間之 Cookie 與網路信標(web beacons)）蒐集之數位資訊。客戶提供資訊予 IBM 時，如需通知個人或取得其同意者，客戶應為通知並取得同意[276]。

4. 「本合約」或依其所為之任何交易，不為任何第三人創設權利或訴因。除非法律禁止以合約拋棄或限制，任一方均不得於訴訟事由發生逾二年後，就「本合約」所生及相關事由提出法律訴訟。任一方均毋須就其無法控制之因素致無法履行之非金錢給付義務而負責。任一方主張他方未履行其義務前，均應給予他方合理補正之機會[277]。

5. IBM 得使用全球各地之人員與資源（包括承包商）支援「IBM 雲端服務」。客戶對「雲端服務」之使用可能使「內容」（包括個人資料）進行跨境傳輸。適用「交易文件」內含一份清單，其中列有為執行「IBM 雲端服務」而可能將「內容」傳輸至及進行處理之國家。BM 負責依「本合約」履行其義務，即使 IBM 使用第三人承包商亦然，且 IBM 仍會與其簽訂適當合約以履行「IBM 雲端服務」之義務[278]。

6. 本公司得提供其他客製化服務、系統配置服務或其他服務以支援「雲端服務」，參考「交易文件」[279]。

---

[276] 同前註，9. 通則 d. 業務聯絡與帳戶使用資訊。

[277] 同前註，9. 通則, i. 訴因。

[278] 同前註，9. 通則, j. 全球資源。

[279] 同前註，9. 通則, k. 其他服務。



DOI:10.6814/NCCU202101656

## 第二項 IBM 資料安全及隱私權政策說明

在 IBM 的合約中對於資料保護的另一份主要文件就是「IBM 資料安全及隱私權政策(Data Security and Privacy Principle)」(簡稱 DSP)。這份文件是 IBM 雲端服務關於資料保護與資訊安全管理的辦法，其中以「資料保護」、「安全政策」、「合規準則」、「資安事件」、「實體安全與門禁管制」、「存取、人為介入、傳輸及隔離控制」、「服務完整性與可用度控管」項目最為重要。摘要說明如下:

一、資料保護

除 IBM 員工、承包商及供應商（包括轉包商）因交付「IBM 服務」所必要者外，不得將「內容」揭露予他人。各「IBM 服務」之安全及隱私權措施之施行，係為保護「IBM 服務」所處理之「內容」，以及為依所適用之 IBM 與「客戶」所訂書面契約（包括「IBM 服務文件」）規定維護該「內容」之可用性，而依 IBM 安全及隱私權設計常規為之。「IBM 服務」專屬之其他安全及隱私權資訊，或載明於相關「IBM 服務文件」，或其他用以協助「客戶」對其是否適合使用「IBM 服務」進行起始及後續評估之標準說明文件[280]。

二、安全政策

IBM 將維護及遵守書面 IT 安全政策及作法，此等政策及作法係為 IBM 業務不可或缺之一部分，且為 IBM 全體員工須遵循之規定。IBM Chief

[280] IBM，IBM 資料安全及隱私權政策(DSP)，https://www.ibm.com/support/customer/csol/terms/#detail-document， 3.資料保護。



DOI:10.6814/NCCU202101656

Information Security Officer 對此負責並執行監督，包括正式規範與修訂管理、員工教育訓練及法規遵循。IBM 對其 IT 安全政策每年應至少審查一次，並於 IBM 認為為保護「IBM 服務」及「內容」之必要時修訂 IT 安全政策。IBM 員工每年須完成 IBM 安全及隱私權教育，並每年保證其確實遵循「IBM 業務行為準則」所訂 IBM 業務行為道德、機密及安全政策等之規定。於 IBM 之本「IBM 服務」作業及支援範圍內，對於「元件」具有其角色專屬職責而被授與特許存取權之人員，將施行其他訓練，此外，為維持相關「IBM 服務文件」所載明之法規遵循及認證者，亦需施行該訓練[281]。

三、合規準則

就標準（非客製）「IBM 雲端服務」而言，IBM 於各「IBM 雲端服務」內所施行及維持之措施，係依 ISO 27001 及/或 SSAE SOC 2[282] 法規遵循年度認證之規定，惟「IBM 服務文件」另有規定者不在此限。IBM 應依「IBM 服務文件」規定，持續遵循「IBM 服務」維持認證。IBM 應依要求出具前述所定法規遵循與認證之證明，例如：經認證獨立第三人稽核所核發之認證、證明文件或報告（應依相關標準所定頻率進行認證獨立第三人稽核）。IBM 於交付或支援「IBM 服務」時採用承包商或供應商（包括轉包商），前揭資料安全及隱私權措施，仍應由 IBM 負責[283]。

四、資安事件

[281] 同前註，4.安全政策。

[282] Atlantic.net，SSAE 16, SSAE18, SOC 1, SOC2: What they are and why you should care，https://www.atlantic.net/hipaa-compliant-hosting/ssae-16-soc-1-soc2-care/ ，最後瀏覽日 2021 年 9 月 18 日。

[283] IBM，前揭註 280， 5.合規準則。



DOI:10.6814/NCCU202101656

IBM 將依「美國商業部國家標準與技術機構 (NIST)) 準則」或相當之電腦安全事故處理之業界標準，維護及遵守採用所規定之事故因應政策，並遵循所適用之 IBM 與「客戶」所訂書面契約之資料外洩通知條款。IBM 應調查其所察覺之「安全事故」，並於「IBM 服務」範圍內，擬定及執行妥適之因應計劃。「客戶」得透過「IBM 服務」專屬事故通報程序（如「IBM 服務文件」所示者）提出申請，無該程序者，則提出技術支援申請，通知 IBM 可疑漏洞或事故。IBM 於其知悉或合理懷疑有足以影響「客戶」之「安全事故」時，將適時通知「客戶」。IBM 將為「客戶」提供合理要求之資訊，例如前項「安全事故」及 IBM 所為補救及還原行動之狀態等相關資訊[284]。

五、實體安全與門禁管制

為防範用以代管「IBM 服務」之由 IBM 管理之設施（資料中心）遭受未獲授權之進入，IBM 將設置適當之實體門禁管制設施，例如：屏障、卡控入口、監視器及真人接待櫃台。前揭資料中心輔助入口，例如：交貨區及運貨區，將予以管制，並與運算資源隔離。由 IBM 管理之資料中心及其內部管制區之出入，應以工作職責所需為限，並應取得授權許可。前揭出入應予記錄，所記錄資料之保留期間不得少於一年。於授權員工離職時，IBM 將撤銷其出入 IBM 管理之資料中心之權限。IBM 採用有正式書面記錄事項之離職手續，包括立即將其從門禁管制名冊中除名，以及繳回實體出入識別證。取得暫時許可以進入由 IBM 管理之資料中心設施或其內部管制區之人員，於其進入相關處所時應予登記，並於登記時要求其出具身分證明文件，且應由授權人員陪同。暫時性出入授權許可（包括送貨許可）應

[284] 同前註，6.資安事件。



DOI:10.6814/NCCU202101656

事先排程，並經授權人員許可。IBM 將採取預防措施，防範由 IBM 管理之資料中心設施之實體基礎架構遭受天然或人為之環境威脅，例如：過高環境溫度、火災、水災、濕度、遭竊及蓄意破壞[285]。

六、存取、人為介入、傳輸與隔離控制

IBM 應保留所記載之「元件」安全架構相關資訊。IBM 於實作前述安全架構前，將各別審查包括專為防範對系統、應用程式及網路裝置所為未獲授權之網路連線而設計之措施，以確認其是否符合深度標準之安全分區、隔離及防禦等規定。IBM 於其維護及支援「IBM 服務」及其相關「元件」時，可能會使用無線網路技術。前述無線網路應予加密，並應要求施行安全識別，且不得允許直接存取「IBM 雲端服務」網路。「IBM 雲端服務」網路不採用無線網路技術 (將以實體線路為標準)[286]。

IBM 將持續進行各項「IBM 服務」措施，此等措施之設計，旨在以符合邏輯之方式隔開及防範「內容」曝露於未獲授權之人或遭其存取。IBM 對正式作業與非正式作業環境應進行適當隔離，「內容」如係傳輸至非正式作業環境者（例如：為依「客戶」要求重製錯誤），該非正式作業環境中之安全及隱私權保護措施應同於正式作業環境。IBM 於經由公用網路傳輸「內容」及啟用加密通訊協定（例如：HTTPS、SFTP 或 FTPS 等通訊協定）時，將非預定用於公用檢視或未經鑑別檢視之「內容」加密，使「客戶」得以經由公用網路，以安全之方式將內容傳輸至「IBM 服務」或從「IBM 服務」傳輸內容。IBM 將依「IBM 服務文件」之規定，將處於靜止狀態之

[285] 同前註， 7.實體安全與門禁管制。

[286] 同前註， 8. 存取、人為介入、傳輸及隔離控制。



DOI:10.6814/NCCU202101656

「內容」加密。若「IBM 服務」包含加密金鑰之管理，IBM 將保留針對安全金鑰之產生、核發、散布、儲存、輪換、撤銷、回復、備份、銷毀、存取及使用所記載之各項程序。

IBM 如需存取「內容」以提供「IBM 服務」，且該存取權限由 IBM 管理者，IBM 應將該存取限制為所需最低層級。前述存取權，包括基礎「元件」管理存取權（特許存取權），應以個人、職責為依據，並應由授權 IBM 人員依權責劃分原則核准及定期驗證之。IBM 將持續施行相關措施，確認並移除具有特許存取權之冗餘帳戶及靜止帳戶，於帳戶所有人離職或授權 IBM 人員（例如：帳戶所有人之經理）提出要求時，應即撤銷該存取權。

依業界標準，及在各「元件」原本即支援之情形下，IBM 將採取相關技術措施，強制非作用中階段作業逾時、多次連續登入嘗試失敗後鎖定帳戶、高保護性密碼或通行詞組識別、密碼變更頻率等措施，以及要求以安全方式傳輸及儲存該等密碼及通行詞組之措施。IBM 將監控特許存取權之使用，並採取為下列用途設計之安全資訊及事件管理措施：(1) 識別遭受未獲授權之存取及活動；(2) 協助進行即時且適當之因應；及(3) 啟用內部及獨立第三人稽核，確認是否遵循所記載之 IBM 政策。

記錄特許存取權及活動之日誌，遵循 IBM 全球記錄管理計劃之規定予以留存。IBM 將採取特定措施，用以防範該等日誌遭受未獲授權之存取、修改及意外或蓄意毀損。在原生裝置或作業系統功能可支援之範圍內，IBM 將對其終端使用者系統採取運算防護措施，包括但不限於端點防火牆、全磁碟加密、簽章型惡意軟體偵測及移除、時間型螢幕鎖定，以及用以執行安全配置及修補要件之端點管理解決方案。依 NIST 的媒體淨化準則，IBM 對預定重複使用之實體媒體為重複使用前，將以安全之方式予以淨化，



DOI:10.6814/NCCU202101656

對非預定重複使用之實體媒體，則予以銷毀。

七、服務完整性與可用度控管

IBM 將執行以下各項：(1) 每年至少執行一次其「IBM 服務」之安全與隱私權風險評估；(2) 於正式作業發布前，及其後至少每年執行一次「IBM 服務」之安全測試及漏洞評量；(3) 請求合格獨立第三人、IBM X-Force™ 或其他合格測試服務提供者（若載明於「IBM 服務文件」）每年至少執行一次「IBM 雲端服務」滲透測試；(4) 依據業界安全配置實作典範，執行「IBM 服務」基礎「元件」自動化漏洞掃描；(5) 依據相關風險、不當運用及影響，補救安全測試與掃描所發現之已識別漏洞；及 (6) 執行「IBM 服務」之測試、評量、掃描及進行補救活動時，應採取適當步驟，以免「IBM 服務」中斷[287]。

IBM 應於「IBM 服務」範圍內，持續採取專為下列用途設計之措施：對「IBM 服務」及關聯系統、網路、應用程式及基礎「元件」進行評量、測試及套用資訊安全建議修補程式。IBM 於其判斷資訊安全建議修補程式為適用且適當時，將依所記載之嚴重性及風險評估準則（以修補程式「一般漏洞評分系統」評比為其依據）實作該修補程式。資訊安全建議修補程式之實作，應受 IBM 變更管理政策之拘束。

IBM 將持續執行專為管理有關將變更應用至「IBM 服務」所致相關風險而設計之政策及程序。對「IBM 服務」所為之變更，包括其系統、網路及基礎「元件」，於其施行前，將先於登錄變更要求中記載之，該要求會載

[287] 同前註，9.服務完整性與可用度控管。



DOI:10.6814/NCCU202101656

明變更之說明與原由、施行細節及時程、敘明對「IBM 服務」及其客戶所生影響之風險說明書、預期成果、回復計劃，以及授權人員之書面核准。IBM 將留存其操作「IBM 服務」時所使用之一切資訊技術資產之清冊。IBM 將持續監視及管理本「IBM 服務」及基礎「元件」之性能（包括容量）及可用度。

將透過以指明重要商業功能並設定其優先順序為預定用途之適當業務衝擊分析與風險評估，分別評量各「IBM 服務」之業務持續及災難回復要件。在前述風險評估保證範圍內之各「IBM 服務」，依業界標準常規，針對其業務持續及災難回復計劃，分別予以界定、記載、保留及每年驗證。「IBM 服務」之回復點及時間目標（如有載明於相關「IBM 服務文件」），將依「IBM 服務」之架構及預定用途等考量定之。實體媒體（例如：內含備份檔之媒體）如有傳送至離站儲存體之需要，傳送之前將對該等媒體施以加密。

### 第三項 小結

本節以 IBM「雲端服務合約」及「IBM 資料安全及隱私政策」為實例說明。「雲端服務合約」架構中的九個項目建立了委託者與受託者在服務中需要負擔的責任。在「內容及資料保護」的條款中的「IBM 資料安全及隱私政策」是「雲端服務合約」對於個資保護的重要依據，故「IBM 資料安全及隱私政策」也有內容摘要。從實例的了解，將有助於在下一節將 IBM 的委外雲端服務文件與銀行業和保險業在使用委外雲端服務時須遵守的法規進行比對，該比對可以檢視出 IBM 的合約對於法規滿足程度。國際型雲端服務廠商在資訊安全與個人資料保護方面多半有通過國際性認證，這些認證對於金融機構在評估風險或準備審核資料時都有助益。



DOI:10.6814/NCCU202101656

# 第三節 從個人資料保護之觀點檢視 IBM 雲端服務合約條款

本文認為金融機構與委外雲端服務業者屬委託機關(資料管理者)與受託機關(受託者)的關係。本節以前節所述「IBM 雲端服務合約」和「IBM 資料安全及隱私政策」為對象，以個資法、個資法施行細則和委外辦法來檢視該文件在個人資料資保護上的符合程度。

## 第一項 與個資法及個資法施行細則之檢視

### 一、個資法部分

此部分以個資法第 4 條及第 27 條第 1 項的規定為主要比較對象。。

從個資法第 4 條來檢視「雲端服務合約」，在「內容及資料保護」中敘述「IBM 雲端服務」所處理資料由客戶或其授權之使用者所提供、授權存取或輸入。也載明客戶授與 IBM、其關係企業及其等之承包商行為提供「IBM 雲端服務」而使用、提供、儲存及以其他方式處理客戶資料。「通則」中說明 IBM 僅作為資訊技術提供者。以上的敘述可以推導出 IBM 對於雲端服務所認定的地位是受託者，接受資料與提供服務都是在為委託機關的授權下進行。

個資法第 27 條第 1 項關於非公務機關保有個人資料檔案應採行適當的安全措施以防止個人資料遭到竊取、竄改、毀損、滅失或洩漏等事故。「雲端服務合約」的「內容及資料保護」中載明「d. 資料保護:「IBM 資料安全與隱私權政策」(IBM Data Security and Privacy Principles (DSP))（網址：http://www.ibm.com/cloud/data-security）適用於正式發佈之標準「IBM 雲端



DOI:10.6814/NCCU202101656

服務」。e. IBM 資料處理附錄: 若有適用 i) 歐洲一般資料保護規章 (EU/2016/679) 或 ii) http://www.ibm.com/dpa/dpl 所載明之其他資料保護法之情形，則於其適用的範圍內，「內容」所含個人資料適用前揭 DPA[288] 及所適用之「DPA 附件」。」為對應個資法第 27 條第 1 項的合約條款。「IBM 資料安全與隱私權政策」對於個資法第 27 條第 1 項的中所指適當安全措施有具體說明，該文件大部分內容都可以對應到安全措施的範圍。

二、個資法施行細則部分

此部分主要以個資法施行細則第 8 條、第 12 條來檢視。

個資法實行細則第 8 條是指委託他人蒐集、處理或利用個人資料時，委託機關應對受託者為適當之監督，並就其應包含的監督事項在條文中例示。此外，該條也明定受託者只能就委託機關的指定範圍進行資料的蒐集、處理和利用，而發生違反有關個人資料保護的相關法律或法規命令時應立刻通知委託機關。就「雲端服務合約」而言，僅針對「委託關係終止或解除時，個人資料載體之返還，及受託者履行委託契約以儲存方式而持有之個人資料之刪除」，在合約「內容及資料保護」對於資料移除有相關條款，並在「合約期間與終止」對於個資的移轉、返還及刪除有原則上的敘述。

「IBM 資料安全與隱私權政策」對應上述施行細則規定是在「合規準則」中將「IBM 於交付或支援『IBM 服務』時採用承包商或供應商（包括轉包商），前揭資料安全及隱私權措施，仍應由 IBM 負責」，以及「資安事件」中所列關於安全事故通報機制，對應個資法實行細則第 8 條有關「受

[288] 請參照「IBM 資料處理附錄」(DPA) 網址 http://ibm.com/dpa。



DOI:10.6814/NCCU202101656

託者或其受僱人違反本法、其他個人資料保護法律或其法規命令時，應向委託機關通知之事項及採行之補救措施。」，可知當 IBM 或是其合作廠商在發生與客戶資料相關的安全事件時，IBM 都有通報客戶的責任。

至於個資法施行細則第 12 條主要是規範在個資法中所出現「適當安全維護措施」、「安全維護事項」、「適當之安全措施」等要求時需要包括項目有哪些。該條文中總共例示十一項措施，執行者可以依適當比例原則落實措施以達到個資保護的目的。

在合約架構上，「雲端服務合約」是用以確立委託機關和受託者之間的責任關係，其中「內容及資料保護」的條款均屬於原則上的敘述。對於安全維護措施需要涵蓋的事項則以「IBM 資料安全與隱私權政策」說明。

「IBM 資料安全與隱私權政策」屬「雲端服務合約」的「內容及資料保護」中載明適用於合約的文件。這份文件詳細記載了安全維護措施的作法。檢視該文件後可以對比出以下的結果:

| | |
|---|---|
| 「IBM 資料安全與隱私權政策」 | 個資法施行細則第 12 條第 2 項 |
| 「資料保護」 | 二、界定個人資料之範圍 |
| 「安全政策」 | 一、配置管理之人員及相當資源<br>五、個人資料蒐集、處理及利用之內部管理程序<br>六、資料安全管理及人員管理 |



DOI:10.6814/NCCU202101656

| | |
|---|---|
| | 七、認知宣導及教育訓練 |
| 「合規準則」 | 三、個人資料之風險評估及管理機制<br><br>九、資料安全稽核機制<br><br>十一、個人資料安全維護之整體持續改善 |
| 「資安事件」 | 四、事故之預防、通報及應變機制 |
| 「實體安全與門禁管制」 | 八、設備安全管理 |
| 「存取、人為介入、傳輸及隔離控制」 | 六、資料安全管理及人員管理<br><br>十、使用紀錄、軌跡資料及證據保存 |
| 「服務完整性與可用度控管」 | 十一、個人資料安全維護之整體持續改善 |

由上述結果可以得知「IBM 資料安全與隱私權政策」對於個資法施行細則第 12 條中所列出「適當安全維護措施」的涵蓋度是足夠的。不過，實務上委託機關仍應以「交易文件」加強在適當安全維護措施上的細節或是合約中未能滿足的部分。

## 第二項 與金融機構作業委託他人處理內部作業制度及程序辦法之檢視

關於以委外辦法檢視「IBM 雲端服務合約」和「IBM 資料安全及隱私政策」的重點是以第 19 條之 1 與第 19 條之 2 作為標準。



DOI:10.6814/NCCU202101656

一、以第 19 條之 1 檢視「IBM 雲端服務合約」和「IBM 資料安全及隱私政策」。

第 19 條之 1 第 1 款規定在委外雲端服務前應對要委託的業務進行委託後的風險有完整的評估，進而對所評估出來的風險有適當的管理，包括對服務品質的確保及單一雲端服務業者。該項規定較偏向對委託機關的要求，屬於委託機關對委外作業風險評估的一環。對受託者而言，「雲端服務合約」中並無相關條款對應。在「IBM 資料安全及隱私政策」的「服務完整性與可用度控管」有敘述 IBM 會對雲端服務提供如安全與隱私權風險評估、安全測試及漏洞評量、滲透測試、依照業務衝擊分析與風險評估制定業務持續及災難回復計劃等，故委託機關在進行風險評估時可以依照受託者所承諾提供的資安服務來判斷。

第 19 條之 1 第 2 款規定金融機構的最終監督義務及應具有專業技術與資源去監督雲端服務業者或委託專業第三人輔助監督作業。該項規定載明金融機構使用委外雲端服務時所負擔的責任程度及監督能力。由於此一規定也偏向對於金融機構的要求，因此在「雲端服務合約」中並無相關條款對應。值得注意的是，在「IBM 資料安全及隱私政策」的「合規準則」中，關於雲端服務擁有 ISO 27001 及/或 SSAE SOC 2 法規遵循年度認證或是可以提供經認證獨立第三人稽核所核發之認證、證明文件或報告。但是這些認證並不等同於該法規所要求委託機關本身或是請專業第三人輔助監督作業，因為不論 ISO 或 SSAE 均非由金融機構所委託。關於這項規定須在「交易文件」中補充委託機關可以對受託人進行監督查核或自行委託專業第三人輔助監督作業。

第 19 條之 1 第 3 款規定委託機關要能確保本身、主管機關和中央銀行



DOI:10.6814/NCCU202101656

均可對雲端服務業者取得執行受託作業的相關資訊，包括客戶資訊、系統查核報告以及實地查核權力。這項規定在「雲端服務合約」及「IBM 資料安全及隱私政策」都「無」可對應的條款，所以必須要在「交易文件」中訂定條款確保資訊的取得及實地查核的可執行。實地查核的發動者包含委託機關、主管機關和中央銀行也需列入條款中。關於實地查核的部分，IBM 的委外雲端服務因為在我國有實體的機房，可執行性較高。大型雲端服務業者目前除 Google 在我國彰濱工業區有實體機房外，其他如微軟的 Azure[289]或是 Amazon AWS 的服務目前在我國僅有當地配合的電信廠商或資訊系統廠商以機房做為雲端服務入口，並非所提供雲端服務的實體機房，所以執行上需在文件中明訂。

第 19 條之 1 第 4 款規定金融機構可以自行委託或與其他委外同一家雲端服務業者的金融機構聯合委託的方式對雲端業者的查核，並明列查核作業應符合規定。該項規定與第 19 條之 1 第 2 項有關專業第三人輔具監督的意義相同，對查核作業的執行有更明確的規定。在「雲端服務合約」及「IBM 資料安全及隱私政策」對於該條文都無可對應的條款，所以必須要在「交易文件」中訂定條款使受託者配合查核作業。關於查核作業的規定是對委託機關在查核作業上應涵蓋的範圍及對於委託執行查核第三方的適格性。這些規定原則和執行細節應載明於委託機關與所委託執行查核的第三方間的合約中。

第 19 條之 1 第 5 款規定是關於金融機構與雲端服務業者在資料傳輸和

[289] 台灣微軟於 2020 年 10 月宣布將於台灣建置 Azure 全球第 66 座區域級（DataCenter Region）雲端資料中心，不過尚未公布詳細的上線時程。相關資訊可以參考以下網址: https://www.ithome.com.tw/news/140741 、https://www.ithome.com.tw/news/140716 ，最後瀏覽日：2021 年 6 月 3 日。



DOI:10.6814/NCCU202101656

儲存時應對資料加密或去識別化等有效保護措施，並應訂定加密金鑰管理機制。在「雲端服務合約」無可對應的條款，但在「IBM 資料安全及隱私政策」的「存取、人為介入、傳輸及隔離控制」中對於資料的傳輸加密及資料加密有對應的條款。關於傳輸加密有列舉可採用的加密方式，對於內容加密並未區分是加密或去識別化，而金鑰管理是採用 IBM 的管理程序而非客戶自訂。

第 19 條之 1 第 6 款規定委託機關對於對資料應保有完整所有權，並應確保雲端服務業者沒有存取客戶資料的權限及做委託範圍以外的利用。在「雲端服務合約」的「內容及資料保護」有相關條款:「本公司、其關係企業及其等之各別承包商僅得以提供及管理「IBM 雲端服務」之目的存取及使用「內容」。本公司同意除 IBM 員工及承包商因交付「雲端服務」所必要者外，不得將「內容」揭露予他人。」。這是對於 IBM 及相關提供雲端服務的單位可以存取客戶資料的聲明，也聲明對於客戶資料需保密。「IBM 資料安全及隱私政策」的「資料保護」中有「除 IBM 員工、承包商及供應商（包括轉包商）因交付「IBM 服務」所必要者外，不得將「內容」揭露予他人。各「IBM 服務」之安全及隱私權措施之施行，係為保護「IBM 服務」所處理之「內容」，以及為依所適用之 IBM 與「客戶」所訂書面契約（包括「IBM 服務文件」）規定維護該「內容」之可用性，而依 IBM 安全及隱私權設計常規為之。」這是對於受託人在執行業務時需資料保密與只能在契約規定下使用客戶資料的規定。此外，在「存取、人為介入、傳輸及隔離控制」中關於權限管理的敘述:「IBM 如需存取「內容」以提供「IBM 服務」，且該存取權限由 IBM 管理者，IBM 應將該存取限制為所需最低層級。前述存取權，包括基礎「元件」管理存取權（特許存取權），應以個人、職責為依據，並應由授權 IBM 人員依權責劃分原則核准及定期驗證



DOI:10.6814/NCCU202101656

之。」是根據人員職權劃分最小權限的管理方式。

第 19 條之 1 第 7 款規定金融機構委託雲端服務業者處理或儲存資料的地點以我國境內為原則，境外為例外。並規定境外地點的決定權、境外地點的法規水準、例外作法為核准制、重要資料備份應在我國等。「雲端服務合約」及「IBM 資料安全及隱私政策」對於該條文都無可對應之條款。僅在「雲端服務合約」的「通則」說明可以在「交易文件」中提供「為執行「IBM 雲端服務」而可能將「內容」傳輸至及進行處理之國家」。此項條文的規定必須以「交易文件」補充才能達成。

第 19 條之 1 第 8 款規定金融機構運用委外雲端服務時，對於服務可能發生中斷的風險要有應變計畫，當決定終止或結束作業委託時，要能將委託作業順利移轉或是移回自行處理。須確保原受託雲端服務業者留存資料全數刪除或銷毀並留存刪除或銷毀記錄。「雲端服務合約」及「IBM 資料安全及隱私政策」對於該條文都無可對應的條款。「雲端服務合約」在合約終止部分的條款大都只說明如何依照通知流程終止合約，對於資料的處理並未說明。「IBM 資料安全及隱私政策」同樣也欠缺該條文所要求關於結束委外服務時的資料移轉及刪除等條款，僅提供「依業界標準常規，針對其業務持續及災難回復計劃，分別予以界定、記載、保留及每年驗證。」的方式給欲委託機關在訂定應變計畫時的參考。此項條文的規定必須以「交易文件」補充才能達成。

二、以第 19 條之 2 檢視「IBM 雲端服務合約」和「IBM 資料安全及隱私政策」。

第 19 條之 2 第 1 項規定金融機構將委外雲端服務的業務具重大性或是要在境外處理時，向主管機關申請核准所需檢具的書審資料。所需檢



DOI:10.6814/NCCU202101656

具的書審資料共具五款，其中以作業委外計畫書的內容規定最多。委外計劃書需涵蓋風險評估及管理機制、資訊安全及管理、雲端服務業者處理受託作業資訊之範圍及方式、確保實地查核權力之說明、緊急應變計畫及退場機制等。這些文件是對於第 19 條之 1 中各項規定的審核依據。「雲端服務合約」及「IBM 資料安全及隱私政策」對於該條文都無可對應的條款。較具相關性的部分為「IBM 資料安全及隱私政策」中「合規準則」、「存取、人為介入、傳輸及隔離控制」及「服務完整性與可用度控管」的條款可以做為這些書審文件的輔助資料。

第 19 條之 2 第 2 項規定是關於重大性作業的定義。該規定中所指屬於重大性作業的情形與客戶資料安全、客戶權益及重要營運服務相關為判斷依據。「雲端服務合約」及「IBM 資料安全及隱私政策」對於該條文的相關議題是當個人資料的處理利用和儲存並使用 IBM 的全球性資源模式下，這些服務的所在地點是否在境內，如果是在境外處理是否合於第 19 條之 1 第 7 項的規定。

### 第三項 小結

本節以個資法(第 4 條及第 27 條第 1 項)、個資法實行細則(第 8 條、第 12 條)和委外辦法(第 19 條之 1 與第 19 條之 2)來檢視「IBM 雲端服務合約」及「IBM 資料安全及隱私政策」對於個資保護的合規程度。檢視的結果可以看出一般委外雲端服務的合約對於個資保護的合規性僅能滿足原則上的規定，較細節的執行方法是需要另外以附件的方式載明才能落實。



DOI:10.6814/NCCU202101656

# 第五章　結論

## 第一節　銀行業與保險業運用雲端服務的趨勢

我國的金融政策向來以穩健發展為方向，對於銀行業及保險業的業務開發及因為業務開發所使用的資訊技術多採取嚴格審查及監理的方式，在銀行業及保險業使用雲端服務的政策上也沒有例外。直到 2019 年，金管會才對於銀行業及保險業使用雲端服務有了明確的法令規範，再加上 2020 年有純網銀、開放銀行、金融上雲等金融政策開始實施，為銀行業及保險業使用雲端服務帶來新的發展契機。

銀行業與保險業使用雲端服務，在法令開放「前」，多半是以「私有雲」的方式做內部系統更新、新科技的導入或是巨量資料分析等，重心擺在引進雲端服務的技術，例如：虛擬化、網絡計算、寬頻網路等將資料處理的資源整合，使資訊的交換與利用更為便利和有彈性。 而法令開放「後」先有聯盟區塊鏈建立的雲端服務，未來對開放銀行的商業活動因為將更為廣泛使用網際網路的相關技術，預期在雲端服務的運用程度上也會大幅增加。除對外部的業務需求，在內部的資訊安全及 IT 維運上也可以運用委外雲端服務，像資料儲存、異地備援、企業持續營運機制等，均可提供銀行業與保險業在經營管理上的經濟效益。

綜觀雲端服務具有商業上可運用的彈性、技術更新速度的優勢、短期投入的經濟效益、配合行動科技發展的趨勢等優點，銀行業及保險業對於雲端服務的運用將持續投入且逐漸增加在營運上的比重，期望未來可以提供更多元及優質的金融服務以達到普惠金融的目標。



DOI:10.6814/NCCU202101656

## 第二節　我國金融監理對雲端服務的態度

我國金融監理機關對於銀行業與保險業使用雲端服務的政策在 2019 年前都是採取「不鼓勵也不禁止」的態度，再加上金融機構的資訊是否可以使用委外雲端服務的並無明文規定，所以金融機構在雲端技術的運用上多半只能與行銷業界合作，使用雲端平台相關的行銷類服務，如：網路問卷調查或是促銷活動等。另外則是以自建「私有雲」的方式進行金融機構內部資訊系統的轉型與開發，並未能廣泛運用委外雲端服務的優勢。金管會的主要疑慮還是在於委外雲端服務對於個人資料保護的完善程度，舉凡金融機購對運用委外雲端服務後的個人資料掌握度不易確定，或是委外雲端服務在個人資料的處理、利用等程序上欠缺透明度等因素，都導致金管會對於委外雲端服務的運用採取審慎態度。

因應與國際金融發展趨勢接軌以及金融科技運用範圍的擴大，金管會在金融政策上也有了相對的調整，從開放銀行、電子保單、保單存摺等，以及因為 COVID-19 防疫所開啟的視訊投保，都可以看出金管會對於金融機構運用委外雲端服務的政策逐漸鬆綁。2019 年 9 月 30 日公告發佈「金融機構作業委託他人處理內部作業制度及程序辦法」部分條文修正後，金融機構運用雲端科技有了明確的法源依據與管理辦法。「委外辦法」的修正也使金融機構運用雲端科技所需遵循的其他法規一起調整，如「保險業作業委託他人處理應注意事項」、「保險業辦理資訊安全防護自律規範」以及「金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法」等。

依據現行規定，金管會對金融機構使用委外雲端服務的監管方式採取雙軌制，也就是依照雲端作業委外的重大性與否區分為「核准制」以及「備查制」。凡具有重大性的委外作業或是將作業委託「境外」業者，都必須採取事先申請核准制，除此之外則採取事後備查制。而委外作業是否具有重大性則必須綜合



DOI:10.6814/NCCU202101656

評估相關因素，包括該項雲端委外作業占總營收比例、對委託機構穩健營運潛在影響、若發生資安問題時對委託機構本身、客戶或市場帶來的影響、委外作業成本與營業成本的佔比，以及委外作業失敗所需付出的風險成本等。除此之外，對於是否涉及境外服務則採實質認定的方式，需視最終提供服務的受託者所在的位置做為判斷的標準。

目前因為委外雲端服務的相關法規剛建立且相關的監理法規也尚未完備，金管會的監理態度仍須觀察。金管會對於使用委外雲端服務的考量應該還是在於資訊安全與個人資料保護的執行狀況，因為雲端服務的維運複雜度、資訊透明度及資訊安全管理能力等，都是影響主關機關「信任度」的因素。金融機構使用雲端服務的發展將取決於雲端服務可運用的彈性與監理機關信任間兩者的平衡。

## 第三節　金融機構運用委外雲端服務的法規議題

銀行業與保險業在運用委外雲端服務時所需要遵守的規範包括「個資法」、「個資法施行細則」、「委外辦法」、「委外注意事項」、「自律規範」及「維護辦法」。其中「個資法」對於委託機構與受託機構的定義尚未明確應該修法增訂。「個資法施行細則」第 8 條與第 12 條對於適當安全措施的所列事項在委外雲端服務上是適用的，而「委外辦法」所增訂的第 19 條之 1 與第 19 條之 2 對於委託機構在運用委外雲端服務的評估、管理、監督、行政流程與書審文件等事項也有適當的涵蓋。但部分規範，如金融機構在委託時有指定資料處理及儲存地點的權力，是否可行則有疑慮; 又如當地資料保護法規不得低於我國要求的規定，但在法規保護高低的明確度上是模糊的，這些規定在執行上的效果均有待觀察。此外，法規所要求檢具的書審資料涵蓋項目廣且審核標準未明確，金融機構恐因準備不易而影響運用委外雲端服務的意願。



DOI:10.6814/NCCU202101656

另一個法律議題是關於委外雲端運用後所帶來的科技成果尚無相關法律配合，例如智能合約因自動履約所產生的交易問題、區塊鏈因資安問題所衍伸的交易有效性、AI的應用是否因資料偏差造成歧視性的決策結果以及AI可以在那些領域使用而在那些領域應該禁止等，這些議題都需要專屬性的法律來處理，因此這部分的發展也應該同步進行。

採用委外雲端服務時必然要用合約來確保雲端業者有效執行各項安全控管措施及保障資料管理者在個人資料保護上的權益。透過委外雲端服務合約範本與金融機構運用委外雲端服務相關規範對照比較，可以說明金融機構與委外雲端業者訂立合約所要具備的架構與條件。委外雲端服務業者在技術上、規模上及市場上的優勢，大多以標準式合約來建立與使用者之間的權利義務關係，標準合約對個資保護多為一般性條款，應透過工作說明書或合約附件對資料服務的執行方式與個資保護機制加以補充，透過技術、流程與管理機制等方式將資訊安全的風險與個人資料保護的效果給予適當的控制，才有適當且符合法規的委外雲端服務。



DOI:10.6814/NCCU202101656

# 參考文獻

## 一、 中文文獻

### (一)專書

Tim Mather, Subra Kumaraswamy, Shahed Latif 著，胡為君譯，(2012)。雲端資安與隱私企業風險對應之道，碁峯資訊股份有限公司。

李顯正，(2020)。保險科技，新陸書局股份有限公司。

林洲富，(2019)。個人資料保護法之理論與實務，元照出版公司。

林鴻文，(2018)。個人資料保護法，書泉出版社。

張陳弘、莊植寧，(2019)。新時代之個人資料保護法制，新學林出版股份有限公司。

黃正傑，(2018)。雲端運算運用與實務，全華圖書股份有險公司。

廖文華、張志勇、蒯思齊，(2021)。雲端運算概論，五南圖書出版股份有限公司。

劉佐國、李世德，(2015)。個人資料保護法釋義與實務，碁峯資訊股份有限公司。

### (二)期刊論文

朱啟恆，(2015)。大數據於金融業之應用，財金資訊季刊(84)，頁 12-18。

林弘斌、鄧介銘，(2017)。淺談區塊鏈技術與金融區塊鏈實作驗證，財金資訊季刊(90)，頁 19-27。

范姜真嫩，(2012)。個人資料自主權之保護與個人資料之合理利用，法學叢刊(225)，頁 69-104。



DOI:10.6814/NCCU202101656

范姜真媺，(2013)。個人資料保護法關於「個人資料」保護範圍之檢討，東海大學法學研究(41)，頁 91-123。

張乃文，(2013)。雲端運算環境之法規遵循議題剖析，科技法律透析，25(7)，頁 21-40。

許銘瑋，(2018)。雲端服務之個人資料保護問題，刑事法雜誌，62(2)，頁 93-161。

陳恭，(2017)。智能合約的發展與應用，財金資訊季刊(90)，頁 33-39。

黃偉倫、林承忠，(2013)。建構安全的雲端運算服務，財金資訊季刊(76)，頁 12-18。

劉定基，(2010)。「個人資料保護法」初論，台灣法學雜誌(159)，頁 1-8。

劉定基，(2014)。雲端運算與個人資料保護-以台灣個人資料保護法與歐盟個人資料保護指令的比較為中心，東海大學法學研究(43)，頁 53-106。

劉定基，(2017)。大數據與物聯網時代的個人資料自主權，憲政時代，42(3)，頁 265-308。

盧韻雅、何翠婷，(2015)。Bank 3.0 及 Digital Bank 帶動金融創新，財金資訊季刊(83)，頁 17-21。

## (三)專書論文

李治安，(2011)。雲端運算相關法律問題初探，財經法新課題與新趨勢。

## (四)學位論文

吳珞齊，(2018)。保險業適用個人資料保護法問題研究-以保險法第 177 條之 1 及個人資料保護法第 3 條為核心，國立政治大學風險管理與保險學系研究所



DOI:10.6814/NCCU202101656

碩士論文。

李曇純，(2018)。我國保險科技的發展，東吳大學法律學系碩士在職專班科技法律組碩士論文。

孫德沛，(2011)。雲端運算時代個資隱私安全之探討-以雲端服務條款為中心，國立政治大學法律科際整合研究所碩士學位論文。

趙偉傑，(2019)。規範制定公私協力之研究—保險業內部控制及稽核監理法治為例，國立政治大學法律學系研究所碩士學位論文。

鄭美華，(2017)。大數據分析與個人資料保護之衝突:從收視行為調查談起，國立政治大學法律科際整合研究所碩士學位論文。

鍾孝宇，(2017)。巨量資料與隱私權-個人資料保護機制的再思考，國立政治大學法律學研究所碩士論文。

## (五)網路資料

AILI，保險業如何透過 AI 革新？我們又如何深陷其中？，網址：https://www.aili.com.tw/message2_detail/56.htm (最後瀏覽日：2021 年 9 月 1 日)。

AWS，雲端儲存，網址：https://aws.amazon.com/tw/what-is-cloud-storage (最後瀏覽日：2021 年 9 月 1 日)。

BINANCE-ACADEMY，私有鏈、公有鏈和聯盟鏈有何區別？，2021 年 4 月 29 日，網址：https://academy.binance.com/zt/articles/private-public-and-consortium-blockchains-whats-the-difference#consortium-blockchains (最後瀏覽日：2021 年 9 月 1 日)。

B 型社會企業，AI 保險讓你理賠不再被刁難...估值 20 億美元的「檸檬汁」(Lemonade) 改寫你對風險的定義 更讓每一筆保費有滿滿的社會關懷，2019 年



DOI:10.6814/NCCU202101656

12 月 15 日， 網址：http://blab.tw/b-media/2019/12/25/ai-20lemonade- (最後瀏覽日：2021 年 9 月 1 日)。

Chen, Sindy，DevOps 介紹 》建立 DevOps 文化，消除開發、營運、品保斷層，CakeResume，2020 年 7 月 6 日， 網址：https://www.cakeresume.com/resources/what-is-devops?locale=zh-TW (最後瀏覽日：2021 年 9 月 1 日)。

CYBAVO，什麼是以太坊？，網址：https://www.cybavo.com/zh-tw/knowledge-center/what-is-ethereum/ (最後瀏覽日：2021 年 9 月 1 日)。

Deloitte 勤業眾信，勤業眾信 Deloitte，《新準則》IFRS 17：保險合約，2017 年 5 月，網址：http://www.ifrs.org.tw/IFRS/NewInfoPDF/N081.pdf (最後瀏覽日：2021 年 9 月 1 日)。

FINANCEDATABIG，銀行 4.0 啟動三零革命，2019 年 3 月 6 日， 網址：https://bigdatafinance.tw/index.php/finance/bank/755-4-0 (最後瀏覽日：2021 年 9 月 1 日)。

IBM，隱私權與安全有何不同，網址：https://publib.boulder.ibm.com/tividd/td/ITPME/SC23-1284-00/zh_TW/HTML/p12plmst18.htm (最後瀏覽日：2021 年 9 月 1 日)。

iThom，面對雲端運算，資訊部門該怎麼做? 2010 年 12 月 28 日， 網址：https://www.ithome.com.tw/node/65236 (最後瀏覽日：2021 年 9 月 1 日)。

iThome，臺灣史上第一次券商集體遭 DDoS 攻擊勒索事件，iThome，2017 年 2 月 14 日， 網址：https://www.ithome.com.tw/news/111875 (最後瀏覽日：2021 年 9 月 1 日)。

Jewel，巨量資料的時代，用「大、快、雜、疑」四字箴言帶你認識大數據，INSIDE，2015 年 2 月 6 日， 網址：https://www.inside.com.tw/article/4356-big-data-1-origin-and-4vs (最後瀏覽日：2021 年 9 月 1 日)。



DOI:10.6814/NCCU202101656

JuiStanley，資料安全與簡單加密演算法見面會 系列 第 24 篇 [Day24] 資料傳輸安全(通道加密)，iThome，2017 年 1 月 8 日， 網址：https://ithelp.ithome.com.tw/articles/10188645 (最後瀏覽日：2021 年 9 月 1 日)。

MBA 智庫，保險核保，2017 年 4 月 11 日， 網址：https://wiki.mbalib.com/zh-tw/%E4%BF%9D%E9%99%A9%E6%A0%B8%E4%BF%9D (最後瀏覽日：2021 年 9 月 1 日)。

MdEditor，Istanbul BFT 解讀(上)，網址：https://www.gushiciku.cn/pl/pEag/zh-tw (最後瀏覽日：2021 年 9 月 1 日)。

中國信託新聞中心，中國信託、陽明海運與奇美實業三方攜手推出國內首例區塊鏈國貿概念驗證，2018 年 5 月 30 日， 網址：http://www.ctbcholding.com/file/news/2018/20180530.pdf (最後瀏覽日：2021 年 9 月 1 日)。

中華人民共和國香港特別行政區政府，採購雲端服務的實務指南，網址：https://www.infocloud.gov.hk/themes/ogcio/media/practiceguideindividual/Practice_Guide(2013-11)_TC_new.pdf (最後瀏覽日：2021 年 9 月 1 日)。

王立恆，要靠數據尋找分行營運新機會，玉山資料科學團隊經驗大公開，iThome，2016 年 10 月 1 日， 網址：https://www.ithome.com.tw/news/108614 (最後瀏覽日：2021 年 9 月 1 日)。

王宏仁，國泰金控如何打造數據生態系？核心架構和關鍵戰略大公開，iThome，2019 年 10 月 4 日， 網址：https://www.ithome.com.tw/news/133440 (最後瀏覽日：2021 年 9 月 1 日)。

王宏仁，微軟宣布在臺 Azure 區域級資料中心，不只 100%用再生能源還要招募 150 人成立 Azure 在地工程團隊，iThome，2020 年 10 月 26 日， 網址：https://www.ithome.com.tw/news/140741 (最後瀏覽日：2021 年 9 月 1 日)。

吳啟彰，巨量資料 (Big data)產業應用成功的關鍵在於速度，不在巨量!，管理知識中



DOI:10.6814/NCCU202101656

心，2015 年 11 月 20 日， 網址：https://mymkc.com/article/content/22243 (最後瀏覽日：2021 年 9 月 1 日)。

李靜宜，【保險公司不再是數據孤島】聯盟鏈將開啟資料共享新時代，iThome，2020 年 8 月 4 日， 網址：https://www.ithome.com.tw/news/139136 (最後瀏覽日：2021 年 9 月 1 日)。

李靜宜，Gartner：數位轉型腳步雖慢，但不出 5 年，AI 將成為保險業主流應用，iThome，2018 年 5 月 31 日， 網址：https://www.ithome.com.tw/news/123542 (最後瀏覽日：2021 年 9 月 1 日)。

李靜宜，中國人壽揭露數位轉型戰略，靠 AI 打造業務員最強武器，iThome，2019 年 6 月 28 日， 網址：https://www.ithome.com.tw/people/131411 (最後瀏覽日：2021 年 9 月 1 日)。

李靜宜，中國信託銀行瞄準新金融時代 3 大機會，將靠 AI、超級個人化以全通路迎戰純網銀，iThome，2020 年 10 月 16 日， 網址：https://www.ithome.com.tw/news/140577 (最後瀏覽日：2021 年 9 月 1 日)。

李靜宜，合庫靠數據驅動數位轉型，要讓資料變成關鍵戰略資產，iThome，2020 年 9 月 24 日， 網址：https://www.ithome.com.tw/people/140102 (最後瀏覽日：2021 年 9 月 1 日)。

李靜宜，金管會公布 2020 年 FinTech 施政重點：開放銀行新階段、數位帳戶未成年開戶、保險區塊鏈上路、純網銀下半年開業，iThome，2020 年 1 月 15 日， 網址：https://www.ithome.com.tw/news/135363 (最後瀏覽日：2021 年 9 月 1 日)。

李靜宜，臺灣第一個區塊鏈支付，台北富邦銀行在政大校園商家成立區塊鏈支付示範區，iThome，2018 年 5 月 14 日， 網址：https://www.ithome.com.tw/news/123145 (最後瀏覽日：2021 年 9 月 1 日)。

李靜宜，銀行資料上雲端，金管會准了！符合條件境外公雲也能用，iThome，2019 年 6 月 27 日， 網址：https://www.ithome.com.tw/news/131515 (最後瀏覽日：



DOI:10.6814/NCCU202101656

2021 年 9 月 1 日)。

李靜宜，銀行資料上雲端哪些新規定？實地查核怎麼做？金管會雲端委外 8 大重點一次看，iThome，2019 年 7 月 5 日， 網址：https://www.ithome.com.tw/news/131678 (最後瀏覽日：2021 年 9 月 1 日)。

沈庭安，【打造臺灣最大銀行區塊鏈平臺】央行終於出手，財金公司串連國內 45 家銀行組區塊鏈平臺，iThome，2016 年 11 月 13 日， 網址：https://www.ithome.com.tw/news/109481 (最後瀏覽日：2021 年 9 月 1 日)。

沈庭安，以太坊區塊鏈技術大突破，臺灣團隊 AMIS 創新區塊鏈共識演算，每秒交易量上看 1,200 筆，iThome，2017 年 7 月 5 日， 網址：https://www.ithome.com.tw/news/115341 (最後瀏覽日：2021 年 9 月 1 日)。

沈庭安，保險理賠與企業融資 2 大智能合約 POC 驗證達成，安侯建業與政大聯手研發區塊鏈應用，iThome，2017 年 3 月 17 日， 網址：https://www.ithome.com.tw/news/112796 (最後瀏覽日：2021 年 9 月 1 日)。

沈庭安，區塊鏈跨產業應用現身，iThome，2016 年 10 月 29 日， 網址：https://www.ithome.com.tw/news/109176 (最後瀏覽日：2021 年 9 月 1 日)。

周新健，R3 聯盟 Corda 運行原理和優劣勢簡析，抹鏈科技，2020 年 7 月 7 日， 網址：https://www.chainnews.com/zh-hant/articles/706633449104.htm (最後瀏覽日：2021 年 9 月 1 日)。

Smart 自學網，網路投保懶人包》疫情期間，有投保需求該怎麼辦？3 分鐘看懂視訊投保、網路投保怎麼做，Smart 自學網，2021 年 6 月 21 日， 網址：https://smart.businessweekly.com.tw/Reading/IndepArticle.aspx?id=6004493 (最後瀏覽日：2021 年 9 月 1 日)。

林妍溱，Google 開源完全同態加密軟體工具，iThome，2021 年 6 月 18 日， 網址：https://www.ithome.com.tw/news/145102 (最後瀏覽日：2021 年 9 月 1 日)。

花俊傑，雲端法規遵循與稽核建議，網管人，2012 年 5 月 22 日， 網址：



DOI:10.6814/NCCU202101656

https://www.netadmin.com.tw/netadmin/zh-tw/technology/7B41372FD1CA4316A8366E50EF111C77 (最後瀏覽日：2021 年 9 月 1 日)。

花俊傑，雲端資料加密與金鑰管理，網管人，2012 年 11 月 14 日， 網址：https://www.netadmin.com.tw/netadmin/zh-tw/technology/0D7370C1E5DC41F59827A3538CC08A85 (最後瀏覽日：2021 年 9 月 1 日)。

金融監督管理委員會，打造數位化金融環境 3.0 全面啟動，2015 年 1 月 13 日， 網址：https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=201501130003&toolsflag=Y&dtable=News (最後瀏覽日：2021 年 9 月 1 日)。

金融監督管理委員會，預告「金融機構作業委託他人處理內部作業制度及程序辦法」部分條文修正草案，2019 年 6 月 27 日， 網址：https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=201906270002&dtable=News (最後瀏覽日：2021 年 9 月 1 日)。

翁芊儒，中信金控揭露未來區塊鏈戰略，聯手兩大國際組織，力推雙平臺瞄準內部金融應用與對外金流服翁芊儒務，iThome，2019 年 12 月 19 日， 網址：https://www.ithome.com.tw/news/134914 (最後瀏覽日：2021 年 9 月 1 日)。

區塊鏈技術指南，同態加密 ，網址：https://poweichen.gitbook.io/blockchain-guide-zh/crypto/homoencryption (最後瀏覽日：2021 年 9 月 1 日)。

國泰金控，AI 下圍棋不稀奇 國泰產險推出 AI 理賠服務，資訊中心，2021 年 6 月 28 日， 網址：https://www.cathayholdings.com/holdings/information-centre/intro/latest-news/detail?news=BdMVl7SEr0OuRoi_LjVXAA (最後瀏覽日：2021 年 9 月 1 日)。



DOI:10.6814/NCCU202101656

國泰金控，國泰產險攜手安侯企管運用保險科技創新技術 - 結合區塊鏈與智能合約提供班機延誤主動理賠，網址：https://www.cathayholdings.com/holdings/information-centre/intro/latest-news/detail?news=h14I3VgFLEmpT5xZbswwhA (最後瀏覽日：2021 年 9 月 1 日)。

帳聯網路科技股份有限公司 AMIS，Istanbul Byzantine Fault Tolerance (IBFT) 共識演算法，網址：https://www.cakeresume.com/companies/amis?locale=zh-TW (最後瀏覽日：2021 年 9 月 1 日)。

張明得，什麼是超融合架構？，iThome，2016 年 1 月 3 日， 網址：https://www.ithome.com.tw/tech/102114 (最後瀏覽日：2021 年 9 月 1 日)。

張家嘯，中信銀布局金融區塊鏈國內首家 R3 聯盟成員，卡優新聞網，2016 年 10 月 12 日， 網址：https://www.cardu.com.tw/news/detail.php?nt_pk=26&ns_pk=30863 (最後瀏覽日：2021 年 9 月 1 日)。

張庭瑜，音樂人的希望！台灣首個區塊鏈音樂發行平台 Soundscape 上線，數位時代，2018 年 1 月 11 日， 網址：https://www.bnext.com.tw/article/47772/kkfarm-soundscape-blockchain (最後瀏覽日：2021 年 9 月 1 日)。

陳奕廷，輕量加密、同態加密與區塊鏈：新世代密碼學的三大聖杯，科學 Online，2018 年 8 月 8 日， 網址：https://highscope.ch.ntu.edu.tw/wordpress/?p=79164 (最後瀏覽日：2021 年 9 月 1 日)。

陳蕙綾，〈觀察〉11 家保險巨頭組成理賠聯盟鏈 Insurtech 浪潮來襲，鉅亨網，2020 年 5 月 10 日， 網址：https://news.cnyes.com/news/id/4474678 (最後瀏覽日：2021 年 9 月 1 日)。

黃郁芸，微軟正式宣布在臺建雲端機房，Azure 最新第八代資料中心設計有哪些特色？，iThome，2020 年 10 月 26 日， 網址：https://www.ithome.com.tw/news/140716 (最後瀏覽日：2021 年 9 月 1 日)。



DOI:10.6814/NCCU202101656

廖婉君，廖婉君觀點：金融科技服務躍上雲端的資安挑戰，風傳媒，2019 年 7 月 15 日， 網址：https://www.storm.mg/article/1467059?mode=whole (最後瀏覽日：2021 年 9 月 1 日)。

沈柏村，ISO 27001 資訊安全標準及驗證流程簡介，金融聯合徵信雙月刊 第十期，2010 年 2 月， 網址：https://www.jcic.org.tw/main_ch/magazinePage.aspx?uid=215&pid=215 (最後瀏覽日：2021 年 9 月 1 日)。

李宗翰，HTTPS 網站居主流 資安重新定義，2014 年 12 月 25 日， 網址：https://www.ithome.com.tw/tech/93108 (最後瀏覽日：2021 年 9 月 1 日)。

樂以媛，如何用合約替雲服務採購把關，政府機關資訊通報第 336 期，2015 年 10 月，網址：https://ws.ndc.gov.tw/Download.ashx?u=LzAwMS9hZG1pbmlzdHJhdG9yLzEwL3JlbGZpbGUvMC85MDc1L2VhZmJhN2FlLTI3MTUtNDBlMC05ZTliLTIzZDBkZDNlMmNjZi5wZGY%3D&n=5aaC5L2V55So5ZCI57SE5pu%2F6Zuy5pyN5YuZ5o6h6LO85oqK6ZecLnBkZg%3D%3D&icon=..pdf (最後瀏覽日：2021 年 9 月 1 日)。

鄭淳伊，走入軟體架構演進史見證微服務發展今昔，網管人，2019 年 4 月 15 日， 網址：https://www.netadmin.com.tw/netadmin/zh-tw/technology/1716C14FB29749B68D8E74C93ACA6263 (最後瀏覽日：2021 年 9 月 1 日)。

顏志仲，金融業資料上雲鬆綁 細說監管作為與技術考量，網管人，2020 年 10 月 28 日， 網址：https://www.netadmin.com.tw/netadmin/zh-tw/viewpoint/959D89FBB3B848E7AE56678D88C60960 (最後瀏覽日：2021 年 9 月 1 日)。



DOI:10.6814/NCCU202101656

## 二、外文文獻

### (一)專書

J.D. Lasica, (2009). Identity in the Age of Cloud Computing: The next-generation Internet's impact on business, governance and social interaction, The Aspen Institute.

John W. Rittinghouse, James F. Ransome, (2010). Cloud Computing Implementation, Management, and Security, CRC Press.

Tim Mather, Subra Kumaraswamy, Shahed Latif, (2009). Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, O'REILLY.

Harry Katzan, Jr., Privacy, (2010). Identity and Cloud Computing, iUniverse.

Renzo Marchini, (2010). Cloud Computing: A Practical Introduction to the Legal Issues, BSi.

### (二)期刊論文

Dimitra Kamarinou, Christopher Millard, and W. Kuan Hon, (2016). Cloud privacy: an empirical study of 20 cloud providers' term and privacy policies -- Part I & Part II, International Data Privacy Law, Vol. 6, No. 2.

### (三)網路資料

Angelo F. Corridori, What is Centralized Computing, 2012, http://zseries.marist.edu/enterprisesystemseducation/zinsights/ECI%20No.%202%20Cent%20Comp%20v2c.pdf (last visited: 1st Sep 2021).

WatElectronic, Cluster Computing: Architecture & Its Types,



DOI:10.6814/NCCU202101656

https://www.watelectronics.com/cluster-computing-architecture-its-types/ (last visited: 1st Sep 2021).

IONOS, Distributed computing for efficient digital infrastructures, https://www.ionos.com/digitalguide/server/know-how/what-is-distributed-computing/ (last visited: 1st Sep 2021).

Jonathan Strickland, How Grid Computing Works, https://computer.howstuffworks.com/grid-computing.htm (last visited: 1st Sep 2021).

Steve Ranger, What is cloud computing? Everything you need to know about the cloud explained, ZDNet, https://www.zdnet.com/article/what-is-cloud-computing-everything-you-need-to-know-about-the-cloud/ (last visited: 1st Sep 2021).

Villanova University, What is Big Data? 18th Jan 2021, https://www.villanovau.com/resources/bi/what-is-big-data/ (last visited: 1st Sep 2021).

Salesforce, Deliver an unforgettable experience using the world's most complete customer service platform, 30th May 2021, https://www.salesforce.com/products/service-cloud/platform/ (last visited: 1st Sep 2021).

Salesforce, What is Marketing Automation, , 30th May 2021, https://www.pardot.com/what-is-marketing-automation/ (last visited: 1st Sep 2021).

Bong De Ungria, SMACIT: Social, Mobile, Analytics, Cloud, Internet of Things, TransFORMe, 29th Jun 2017, https://bongdeungria.com/smacit-social-mobile-analytics-cloud-internet-of-things/ (last visited: 1st Sep 2021).



DOI:10.6814/NCCU202101656

Gartner, IT Governance (ITG), 28th Jun 2021, https://www.gartner.com/en/information-technology/glossary/it-governance (last visited: 1st Sep 2021).

IBM, Cloud Service Agreement, https://www.ibm.com/support/customer/csol/terms/#detail-document, 1. Cloud Service, a. IBM Cloud Services. (last visited: 1st Sep 2021).

IBM, Data Security and Privacy Principle (DSP), https://www-03.ibm.com/software/sla/sladb.nsf/pdf/7745WW2/$file/Z126-7745-WW-2_05-2017_en_US.pdf (last visited: 1st Sep 2021).

IBM, Data Processing Addendum (DPA), https://www.ibm.com/support/customer/csol/terms-pdf/dpa/Z126-7870-02-03-2019-zz-en.pdf (last visited: 1st Sep 2021).

IBM, IBM Privacy Statement, https://www.ibm.com/privacy (last visited: 1st Sep 2021).

IBM, Cloud Service Agreement, https://www.ibm.com/support/customer/pdf/terms/csa_th.pdf (last visited: 1st Sep 2021).

CSRC, Cloud Computing, https://csrc.nist.gov/Projects/Cloud-Computing (last visited: 1st Sep 2021).

David Beach, The Insurtech trends making the greatest impact in 2017, bobsguide.com, 2017, http://www.bobsguide.com/guide/news/2017/Sep/11/the-insurtech-trends-making-the-greatest-impact-in-2017/ (last visited: 1st Sep 2021).

Fred H. Cate, Big Data and the Future of Data Production, 10th Jun 2015, https://www.pcpd.org.hk/privacyconference2015/files/Cate_presentation.pdf



DOI:10.6814/NCCU202101656

(last visited: 1st Sep 2021).

Fred H. Cate, Peter Cullen, Viktor Mayer-Schonberger, Data Protection Principle for 21st Century: Revising the 1980 OECD Guideline. https://www.oii.ox.ac.uk/archive/downloads/publications/Data_Protection_Principles_for_the_21st_Century.pdf (last visited: 1st Sep 2021).





DOI:10.6814/NCCU202101656

# 附錄

## IBM 合約與法規比較

| 法律規範 | 合約相關 | 隱私權政策相關 |
|---|---|---|
| 個資法第 4 條:<br>受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於本法適用範圍內，視同委託機關。 | 2. 內容及資料保護/<br>a. 貴客戶所提供之「內容」: 貴客戶授與本公司、其關係企業及其等之承包商行使下列行為之權利與權限：為提供「IBM 雲端服務」而使用、提供、儲存及以其他方式處理「內容」。<br>b.「內容」之使用: 本公司、其關係企業及其等之各別承包商僅得以提供及管理「IBM 雲端服務」之目的存取及使用「內容」。<br>9. 通則/<br>a. IBM 之契約地位: IBM 僅作為資訊技術提供者。 | 無說明 |
| 個資法第 27 條:<br>第 1 項:非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。 | 2. 內容及資料保護/<br>d. 資料保護:「IBM 資料安全與隱私權政策」(IBM Data Security and Privacy Principles (DSP))（網址：http://www.ibm.com/cloud/data-security）適用於正式發佈之標準「IBM 雲端服務」。<br>e. IBM 資料處理附錄: 若有適用 i) 歐洲一般資料保護規章(EU/2016/679) 或 ii) | 全部與該法條相關 |



DOI:10.6814/NCCU202101656

| | | |
|---|---|---|
| | http://www.ibm.com/dpa/dpl 所載明之其他資料保護法之情形，則於其適用的範圍內，「內容」所含個人資料適用前揭 DPA 及所適用之「DPA 附件」。 | |
| 個資法實行細則第 8 條:<br>委託他人蒐集、處理或利用個人資料時，委託機關應對受託者為適當之監督。<br>前項監督至少應包含下列事項：<br>一、預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。<br>二、受託者就第十二條第二項採取之措施。<br>三、有複委託者，其約定之受託者。<br>四、受託者或其受僱人違反本法、其他個人資料保護法律或其法規命令時，應向委託機關通知之事項及採行之補救措施。<br>五、委託機關如對受託者有保留指示者，其保留指示之事項。<br>六、委託關係終止或解除時，個人資料載體之返還，及受託者履行委託契約以儲存方式而持有之個人資料之刪除。<br>第一項之監督，委託機關應定期確認受託者執行之狀況，並將確認結果記錄之。<br>受託者僅得於委託機關指示之範圍內，蒐集、處理或利用個人資料。<br>受託者認委託機關之指示有違反本 | 2.內容及資料保護: f.「內容」之移除; 相關規定(六)<br>7.合約期間與終止; 相關規定(六) | 5. 合規準則; 相關規定(四)<br>6. 資安事件; 相關規定(四) |



DOI:10.6814/NCCU202101656

| | | |
|---|---|---|
| 法、其他個人資料保護法律或其法規命令者，應立即通知委託機關。 | | |
| 個資法實行細則第 12 條:<br>本法第六條第一項但書第二款及第五款所稱適當安全維護措施、第十八條所稱安全維護事項、第十九條第一項第二款及第二十七條第一項所稱適當之安全措施，指公務機關或非公務機關為防止個人資料被竊取、竄改、毀損、滅失或洩漏，採取技術上及組織上之措施。<br>前項措施，得包括下列事項，並以與所欲達成之個人資料保護目的間，具有適當比例為原則：<br>一、配置管理之人員及相當資源。<br>二、界定個人資料之範圍。<br>三、個人資料之風險評估及管理機制。<br>四、事故之預防、通報及應變機制。<br>五、個人資料蒐集、處理及利用之內部管理程序。<br>六、資料安全管理及人員管理。<br>七、認知宣導及教育訓練。<br>八、設備安全管理。<br>九、資料安全稽核機制。<br>十、使用紀錄、軌跡資料及證據保存。<br>十一、個人資料安全維護之整體持續改善。 | 2.內容及資料保護 | 3. 資料保護:a. b. c. ;相關規定(二)<br>4. 安全政策:a. b. c. d. ;相關規定(一) (五) (六) (七)<br>5. 合規準則:a. b. c. ;相關規定(三) (九) (十一)<br>6. 資安事件:a. b. c. ;相關規定(四)<br>7. 實體安全與門禁管制:a. b. c. d. ;相關規定(八)<br>8. 存取、人為介入、傳輸及隔離控制; 相關規定(六) (十)<br>9. 服務完整性與可用度控管; 相關規定(十一) |
| 委外辦法第 19 條之 1: | 無說明 | 9. 服務完整性 |



DOI:10.6814/NCCU202101656

| | | |
|---|---|---|
| 金融機構將作業委託他人處理涉及使用雲端服務，應依下列規定辦理：<br>一、金融機構應確保作業風險控管，充分評估受託機構處理之風險，採取適當風險管控措施，確保作業委外處理之品質，並應注意作業委託雲端服務業者之適度分散。 | | 與可用度控管 |
| 委外辦法第 19 條之 1:<br>二、金融機構對雲端服務業者負有最終監督義務，並應具有專業技術及資源監督雲端服務業者執行受託作業，並得視需要委託專業第三人以輔助其監督作業。 | 無說明 | 5. 合規準則: a. b. c.<br>8. 存取、人為介入、傳輸及隔離控制: h. |
| 委外辦法第 19 條之 1:<br>三、金融機構應確保其本身、主管機關及中央銀行，或其指定之人能取得雲端服務業者執行受託作業之相關資訊，包括客戶資訊及相關系統之查核報告，及實地查核權力。 | 無說明 | 無說明 |
| 委外辦法第 19 條之 1:<br>四、金融機構得自行委託，或與委託同一雲端服務業者之其他金融機構聯合委託具資訊專業之獨立第三人查核，並應符合下列規定：<br>（一）確認其查核範圍涵蓋雲端服務業者受託處理作業相關之重要系統及控制環節。<br>（二）應評估第三人之適格性，以及其所出具查核報告內容之妥適性並符合相關國際資訊安全標準。<br>（三）應針對金融機構所委託作業 | 無說明 | 無說明 |



DOI:10.6814/NCCU202101656

| | | |
|---|---|---|
| 範圍進行查核並出具報告。 | | |
| 委外辦法第 19 條之 1:<br>五、金融機構傳輸及儲存客戶資料至雲端服務業者，應採行客戶資料加密或代碼化等有效保護措施，並應訂定妥適之加密金鑰管理機制。 | 無說明 | 8. 存取、人為介入、傳輸及隔離控制: d. e. |
| 委外辦法第 19 條之 1:<br>六、對委託雲端服務業者處理之資料應保有完整所有權，除執行受託作業外，金融機構應確保雲端服務業者不得有存取客戶資料之權限，並不得為委託範圍以外之利用。 | 2.內容及資料保護: b.「內容」之使用 | 3. 資料保護: a. b.<br>8. 存取、人為介入、傳輸及隔離控制: f. |
| 委外辦法第 19 條之 1:<br>七、委託雲端服務業者處理之客戶資料及其儲存地以位於我國境內為原則，如位於境外，應依下列規定辦理：<br>（一）金融機構須保有其指定資料處理及儲存地之權力。<br>（二）境外當地資料保護法規不得低於我國要求。<br>（三）除經主管機關核准者外，客戶重要資料應在我國留存備份。 | 9.通則: j.全球資源 | 無說明 |
| 委外辦法第 19 條之 1:<br>八、金融機構應訂定妥適之緊急應變計畫，降低因作業委託而可能有服務中斷之風險。金融機構終止或結束作業委託，應確保能順利移轉 | 無說明 | 9. 服務完整性與可用度控管 e. |



DOI:10.6814/NCCU202101656

| | | |
|---|---|---|
| 至另一雲端服務業者或移回自行處理，並確保原受託雲端服務業者留存資料全數刪除或銷毀，並留存刪除或銷毀之紀錄。 | | |
| 委外辦法第 19 條之 2:<br>金融機構將作業委託他人處理涉及使用雲端服務，具重大性或依第十八條將作業委託至境外者，應檢具下列書件向主管機關申請核准始得辦理：<br>一、依第四條第二項訂定之委外內部作業規範。<br>二、董（理）事會決議之議事錄。但外國銀行在臺分行得由經總行授權人員出具同意書為之。<br>三、法規遵循聲明書。<br>四、作業委託雲端服務業者處理之必要性及適法性分析，其中應包括對雲端服務業者遵守我國客戶資料保護相關規定之評估。<br>五、作業委外計畫書，其內容應包括：<br>（一）風險評估及管理機制：<br>1.應對雲端服務業者進行審查以確保提供作業之可靠性、遵法性，包括對業務持續性、替代性及集中性之分析。<br>2.應具專業技術及資源監督雲端服務業者執行受託作業之說明。<br>（二）資訊安全及管理：<br>1.金融機構對於客戶資料之加密或代碼化、金鑰保管、資料傳輸及區隔，以及資料所有權說明。<br>2.資料儲存地之管理政策，包括資 | 無說明 | 5. 合規準則<br>8. 存取、人為介入、傳輸及隔離控制<br>9. 服務完整性與可用度控管: e. |



DOI:10.6814/NCCU202101656

| | | |
|---|---|---|
| 料處理及儲存於境外時，有關當地法律、政治、經濟安定性評估說明，資料備份及得隨時存取資料之說明。<br>（三）金融機構、主管機關及中央銀行，或其指定之人取得雲端服務業者處理受託作業資訊之範圍及方式，包括取得客戶資訊及相關系統之<br>查核報告，及確保實地查核權力之說明。<br>（四）緊急應變計畫及退場機制，包括金融機構具有充分資源應變及退場之說明。 | | |
| 委外辦法第 19 條之 2:<br>前項所稱具重大性之作業，係指下列情形之一：<br>一、受託作業如無法提供服務或有資訊安全疑慮，對金融機構之業務營運有重大影響者。<br>二、受託作業涉及客戶資料安全事件，對金融機構或客戶權益有重大影響者。<br>三、其他對金融機構或客戶權益有重大影響者。 | 無說明 | 無說明 |
| 委外辦法第 19 條之 2:<br>金融機構將作業委託他人處理涉及使用雲端服務，不屬第一項具重大性或依第十八條將作業委託至境外者，應檢具第一項第三款至第五款之書件，報經主管機關備查。 | 無說明 | 無說明 |



DOI:10.6814/NCCU202101656

| | | |
|---|---|---|
| 委外辦法第 19 條之 2:<br>外國銀行在臺分行及在臺子銀行作業委託總行、母行或所屬集團之分支機構及子公司，複委託雲端服務業者處理，應檢具第一項作業委外計畫書，併同第十八條規定書件向主管機關申請核准，並應依下列規定辦理：<br>一、總行、母行或所屬集團之分支機構及子公司所在地主管機關對作業委託雲端服務業者處理之監理規範不低於我國規定。<br>二、作業委外計畫書內容，得由其總行、母行或所屬集團之分支機構及子公司出具相當性之說明文件代之。 | 無說明 | 無說明 |





DOI:10.6814/NCCU202101656