國立政治大學國際經營與貿易學系碩士班

碩士論文

指導教授：蔡孟佳　博士

論我國導入貿易雲之資訊安全風險暨法規因應

研究生：董玉潔

中華民國一○○年七月

謝辭

這篇論文得以完成，首要感謝恩師蔡孟佳教授。老師在課堂或各種討論時，總不吝分享專業見解、研究方法、以及待人處事的方法，就論文本身，則給予我許多彈性與指導，對我而言，是非常寶貴的收穫！感謝口試委員──林桓教授與李治安教授，撥空給予我許多具體建議與指導，同時分享國貿、科技、法律相關的知識與實務經驗，使我增長見聞，也使這篇論文更加完善。

感謝美亞捷運董事長鮑學超先生、國貿局執行秘書呂素慎女士、介宏資訊業務部經理孫元順先生、以及關貿網路股份有限公司稽核室總稽核魏垚德先生，在百忙中接受我的訪談，使我得到許多實務資訊，能與文獻資料互為參照。感謝瑜君，在我最徬徨時分享許多資訊，使我能及時找到論文的靈感與方向。

在法組的這段期間，除感謝蔡老師的指導，也感謝楊光華老師與施文真老師諸多教誨。楊老師與施老師透過身教與言教，提點我許多學術研究、工作及待人的原則，在課堂上則分享專業見解、寶貴實務經驗，以及生活趣事，讓我獲益良多，非常感謝三位老師的付出！感謝法組的學長姊、同學與學弟妹，特別是與我同甘共苦的怡臻、姿嫻、琇霙、滋立與苔心，感謝你們豐富我在研究所裡的生活！

感謝大學與研究所中每位教導過我的師長，開拓我的視野與思想。感謝研究所的同學，如不是你們幫忙，難以想像我應如何度過每次必修課考試。特別感謝宣伊、褚哥、伊琇、涵屏，在平淡的日子裡帶給我歡笑與驚喜。

感謝高中與大學以來的好友，特別是琪琪、阿鴨、2307 室友、瑞德、圈圈、皓皓、蛇、岷翰、湯圓、迦漪、小多、惠閔、煒迪、均豪、阿龐、柏維、小笨、政大法服、讀書會、藍海計畫、系足，感謝你們與我分享生活諸多喜樂，包容我急躁的脾氣，在我難過或煩躁時帶給我安慰。能認識你們，我實在三生有幸。

感謝支持我的爸爸、媽媽、玉慈、玉明，使我在面對任何糟糕的情況時，都還有你們做為後盾。最後，感謝天父，讓我完成這個階段的一切。

玉潔　2011 年 10 月　台北木柵

摘要

近年來，雲端運算成為我國貿易商理想的電子商務模式。雲端運算基本概念為將資訊和資源集中存放在「雲」上，透過網路服務提供資源，幫助企業提升效率、降低運籌成本。然而，雲端運算的原理造成使用者將資訊存放在網路之某處，使用者無法直接控制其資料，進而衍生出資訊安全之疑慮。也因此，當企業決定是否導入雲端運算時，往往將資訊安全納入考量。若欲鼓勵我國貿易商導入雲端運算，分析資訊安全風險、了解如何管理這類風險，係有其必要性。

本研究主要目的，係為我國貿易商提供較清晰之雲端運算資訊安全分析，包含雲端運算可能之資訊安全風險，以及管理這些風險的方式。依本研究比較分析之結果，雲端運算資訊安全風險與其他電腦或網路產品、服務之資訊安全風險類似，並可透過技術、管理與法律以降低風險。然而資訊安全風險無法被完全去除，在此情況下，貿易商宜透過契約保障其資訊本身、以及相關權利。

關鍵字：貿易商、雲端運算、資訊安全、雲端運算服務契約

The Study of Information Security Risks and Related Legal Instruments on the Cloud Computing of International Trade

Abstract

In recent years, cloud computing has become an ideal way for most Taiwanese trading companies to adopt e-commerce. The basic model of cloud computing is to provide resource in the form of internet service. By centralizing data and resource onto “the cloud”, cloud computing helps companies to improve efficiency with lower budget. However, this approach raises concern about information security, for users’ data will be stored in the internet, rather than being directly controlled by the users. Due to this fact, companies tend to take information security into consideration before moving to the cloud. To encourage Taiwanese trading companies, analyzing and learning how to manage the information security risks are rather necessary.

This research aims to provide a clearer view of the information security to Taiwanese trading companies, including the possible information security risks and the ways to manage these risks. Through comparison and analysis, we conclude that the information security risks of cloud computing and of other computer or internet products or service are similar, and these risks can be reduced by technical methods, management and laws. However, these risks cannot be removed, and in this situation, trading companies are suggested to protect their data and their rights via contracts.

Keywords: Trading companies, cloud computing, information security, cloud computing contract

目錄

表目錄

圖目錄

第一章、緒論

第一節　研究動機

雲端運算係近年來新興之網路服務模式，使用者透過網際網路與簡單的設備，即可取得雲端服務業者提供的服務。雲端服務對商業活動帶來許多好處，譬如幫助企業節省初期投入之成本，與企業分工，使企業得以將其資源集中在發展其主要商業活動，或培養其他競爭優勢。

雲端運算目前仍未被充分運用在我國貿易產業[1]。本研究認為，在眾多電子商務模式中，中小企業導入雲端運算之障礙較低，貿易商導入後可加速貿易流程，達到提升效率之結果，同時也降低運籌成本，這些改變將使貿易商得因應高度國際競爭和廠商自行採購之趨勢。因此，推行貿易雲端，理論上將對我國國際貿易帶來許多好處。

本研究觀察與雲端運算相關的統計資料，發現目前企業對雲端運算最大的顧慮之一為資訊安全[2]。在國際貿易活動中，貿易商的競爭力來源為商機、客源與貨源資訊，屬於貿易商最重要的資產，當貿易商決定是否導入貿易雲端時，資訊安全勢必成為其考量的重要因素，若能使我國貿易商對雲端運算資訊安全相關事項與風險管理有充分認識，或能降低其對雲端運算資訊安全的疑慮，進而提升其導入貿易雲端的意願。基於上述理由，本研究整理並比較資訊安全風險與其管理方式，當中包含透過契約分配資訊安全相關責任，並且提出建議，以使我國貿易商對雲端的資訊安全與相關管理方式有較清楚的認識。

---

[1] 關貿網路，作者訪談內容。

[2] 例如趨勢科技於 2010 年針對六國一般企業中的 1200 名 IT 決策者為調查，發現 43%的企業在過去一年內發生資訊安全問題。此外，有 50%之受訪者認為雲端運算的資訊安全是導入雲端運算的最大障礙。資料來源：趨勢科技研究：43%的受訪企業曾經遇到雲端服務廠商發生資訊安全問題，自由時報電子版，2011 年 6 月 14 日。

第二節　研究目的與方法

本研究主要研究目的為探討貿易商導入貿易雲端時面臨的資訊風險，以及貿易商如何避免、分散或管理這些風險，特別是討論貿易商與雲端運算服務提供者締約時，貿易商有關資訊安全的權益是否能受充分保障。

本研究主要採取的研究方法為文獻之回顧、對業者之訪談，以收集相關參考資料，進而透過比較方式，歸納出雲端運算模式與既有電腦與網路模式（以下簡稱「傳統模式」）產品或服務的差異、資訊安全風險的差異、以及契約內容的差異，進而得出貿易商在導入貿易雲端時應特別注意的資訊安全風險、與相關管理事項。

上述事項之外，本研究因欠缺具體的「貿易雲端」範本，本文中有關「貿易雲端」之概念與模式，係透過目前既有資料與資訊所推測出的結果。我國與其他國家之雲端運算產業尚在發展之中，且無專門針對貿易商或貿易活動建構的雲端運算服務，是以本研究先就貿易商與貿易相關產業之需求，以及雲端運算之模式與特性，假設「貿易雲端」之模式與使用範圍。

第三節　研究架構

本研究第二章介紹貿易活動、雲端運算，同時設定貿易雲端之模式與範圍。因為我國尚未有具體的貿易雲端，本研究考量我國貿易商活動、特性，以就貿易雲端設立適當的模式與架構，達到為貿易商提升效率、降低成本等目標。

第三章探討貿易雲端對貿易商帶來的資訊安全風險，以及消除風險的方法。有關貿易雲端與傳統模式的資訊安全風險，二者之原理與情況大致相同，因此傳統模式的技術或管理方式，可被適用於雲端運算之資訊安全維護，有關電腦或電子商務之國內法律，亦可對雲端運算之資訊安全帶來正面影響。然而，有關維護資訊安全的技術與管理、以及損害發生時由哪一方承擔後果，因各國立法速度不及資訊科技發展，這些事項應仰賴雙方透過契約來分配責任。

第四章探討雲端運算契約如何分配資訊安全的維護責任、以及資訊安全受侵害所導致之損害由誰承擔。本章之討論順序，將先檢討雲端運算既有服務契約中權利義務分配、以及相關責任條款，繼而以之與我國貿易相關的傳統模式契約作一比較。有關我國貿易相關的傳統模式契約，除可取得之具體契約內容之外，資料來源主要來自對資訊業者的訪談內容，從其中瞭解資訊業者過去與貿易商或其他貿易相關業者之交易模式，以及系統損壞或資訊安全發生問題時的解決方式。

第五章就第二章至第四章之觀察結果做出結論，並且針對貿易商導入雲端運算之資訊安全提出建議，其中最主要的一項，是提醒我國貿易商在導入貿易雲端前，應充分了解該貿易雲端服務提供者提供服務與維護資訊安全的方式，以及與服務相關的條款內容，以盡可能地透過契約掌握資訊之傳輸、處理或儲存，確保資訊本身之安全性，倘若資訊安全發生漏洞、造成貿易商受有損失時，締約時對相關條款之瞭解、決策，亦能使貿易商較為充分準備地因應與請求賠償。

本文研究架構如圖 1。

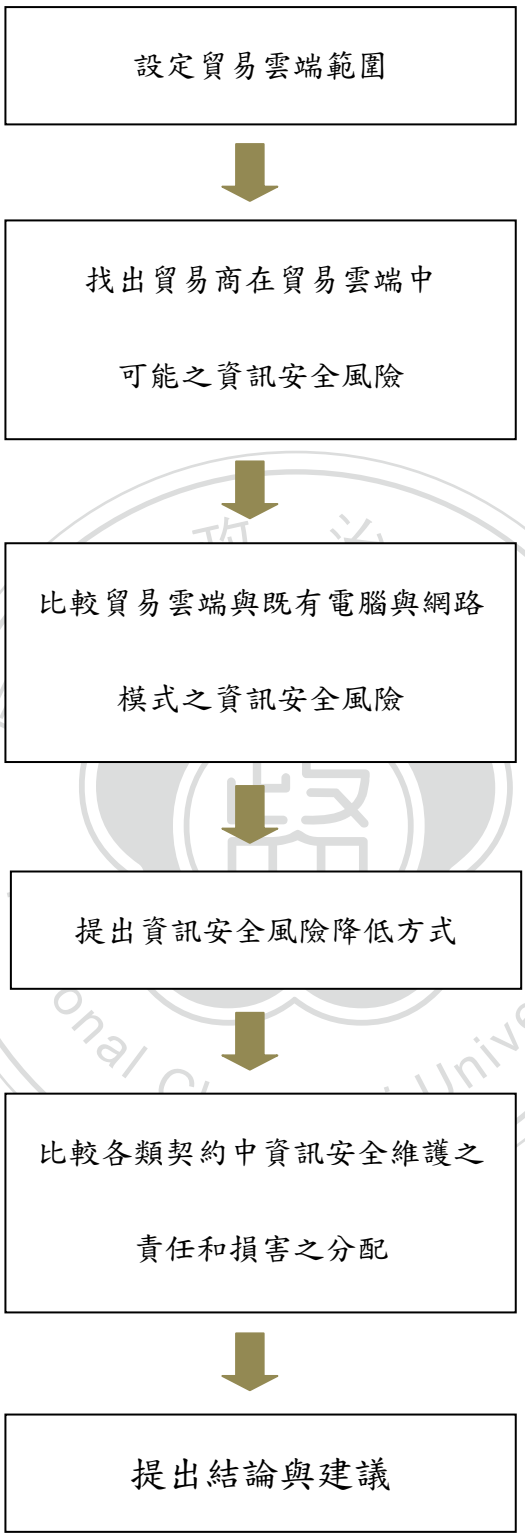

圖 1　本研究架構

資料來源：本研究自製。

第二章、我國貿易活動導入雲端運算

台灣屬於海島型國家，因欠缺自然資源，加上地理位置優越，國際貿易成為發展經濟的主要來源。我國貿易商多為中小企業，在國際自由貿易盛行，加上企業垂直整合、自行發展貿易之趨勢下，貿易商必須尋求改變，以提升競爭力，是以改善貿易流程、提升貿易效率，對我國貿易業者、乃至於我國整體經濟發展，皆是至關重要的工作。

導入電子商務被認為是提升商業效率、降低運籌成本的方法。透過電子商務為交易，係指當事人透過電子與網路等形式進行交易活動。電子商務可被運用在貿易活動的許多環節，譬如透過網際網路為貿易拓展及通訊聯絡，或透過貿易文件通關自動化與無紙化活動，使報關更簡便迅速。依目前情況，我國已導入電子商務的貿易業者，已透過台灣經貿網等網站收集商情與資訊，使用不同軟體開發業者與相關資訊業者的作業系統處理文件與資訊，並得配合經濟部國貿局下之貿易便捷化計畫，以電子方式呈現及遞交各類報關文件。

目前新興起之雲端運算，亦屬於電子商務的類型之一。雲端運算係一正在發展中的概念，大致上可被描述為透過網際網路來管理、處理或儲存資訊。雲端運算具有導入時不需大量成本之優點，適合規模為中小企業的貿易商，專門為貿易打造「貿易雲端」，應可為我國許多缺乏研發能力的中小規模貿易商帶來利益。然而，貿易雲端應提供哪些服務、貿易商應選擇何種導入方式等事項，仍須仰賴對貿易商需求、個別貿易商能力之評估。在我國，貿易雲端仍屬一初步構想，其模式與所欲提供的服務項目仍不明確。

基於前述之認知，本章第一節介紹國際貿易基本知識、相關活動、貿易主體、貿易產業導入雲端運算前的電子商務發展狀況；第二節介紹雲端運算之定義、範圍與特性，並將之與既有的電腦與網路模式做一比較，最後提出本研究導入的貿易雲端內容。

第一節 國際貿易活動暨我國貿易導入電子商務之進展

國際貿易係指國與國之間的交易活動，故具有涉外性與國際性。國際貿易的主體是貿易商，其所負責的工作繁雜瑣碎，且牽涉許多文件或單據交換，譬如進口商透過銀行提供信用狀給出口商，或貿易商依貨品管制措施向政府取得簽證或檢疫證明，或在出進口活動中基本的通關流程，貿易商亦須準備報關的文件。貿易商之外，貿易流程中還包含其他參與者，譬如銀行、物流業者與政府機關。

國際貿易具有跨國界、複雜、多方參與、所涉文件眾多複雜等特性，貿易商與政府可能透過貿易流程之改善、或資訊科技之幫助，以促進貿易活動的效率，因此導入電子商務，對貿易活動將有所助益。雲端運算僅為導入電子商務的一種方式，在雲端運算蓬勃發展之前，我國貿易商已透過網際網路為搜尋與聯繫活動，政府則結合相關業者推行貿易便捷化計畫，這些成果皆屬於電子商務的類型。在討論我國貿易業者應否、或如何導入貿易雲端時，過往電子商務經驗與成果可作為前車之鑒，故本研究將先檢視我國貿易業與貿易業的電子化商務成果，以俾判斷應否導入、以及擬定導入策略。

一、 國際貿易性質、主體與活動

本節介紹國際貿易、其主體與相關活動，以及我國國際貿易與貿易業者的特性，以歸納出我國貿易業者的特徵與需求。

（一） 國際貿易之意義、範圍、特性與活動

國際貿易泛指國與國之間的交易活動，牽涉到不同國家之買賣當事人，以及貨物和款項跨境移動。國際貿易的廣義定義將無形勞務、技術或權利的交易包含

在國際貿易範疇之內，狹義的國際貿易，指的則是有形貨物的國際交易[3]。國際貿易活動具備國際性與涉外性，涉及許多專業知識，包含國際貿易的貨物買賣契約、運送契約、保險契約、融資及外匯處理等事項、各國或國際上相關之規範、規則或國際慣例[4]。國際貿易活動主要包含下列：

1. 貿易開發與拓銷的過程。
2. 貿易磋商與訂約的過程。
3. 辦理進口簽證及申請開發信用狀過程。
4. 接受信用狀及辦理出口融資的過程。
5. 貨物生產與準備交貨的過程。
6. 申請簽證和取得各樣許可或同意文件的過程。
7. 貨物檢驗及辦理公證的過程。
8. 貨物洽運及辦理保險的過程。
9. 貨物申報通關及裝運的過程。
10. 進口貨物驗放及繳稅的過程。
11. 進出口結匯處理的過程。
12. 貿易索賠及糾紛處理的過程[5]。

（二） 國際貿易主體

國際貿易中的主體是貿易商,其為在國際間從事商品買賣活動的公司行號[6]。貿易商主要扮演商業活動中的仲介角色，以自己或他人名義，購入商品後轉售、

[3] 蔡孟佳，國際貿易實務，頁 3，2006 年 7 月 3 版。
[4] 同前註。
[5] 同前註。
[6] 同前註，頁 19。

或提供他人服務賺取佣金[7]。

依貿易商的商業活動，其可被區分為狹義貿易商與廣義貿易商。狹義貿易商係公司本身不從事生產，只從事商品交易，業務內容包含進口業務與出口業務[8]；廣義貿易商，則是公司本身從事貿易活動之外，同時具有其他身分，譬如製造商或生產者，這種情況下，多半是公司在其內部成立進出口部門，或於國外設立分支機構，自行辦理商品之進出口業務[9]。

貿易商被歸類於服務業範疇。依「中華民國行業標準分類」於 2001 年第 7 次修訂，行政院主計處刪除「國際貿易業」，改依其買賣性質，歸入「批發業」或「零售業」下的適當類別[10]。又，依我國「國民所得統計」，批發業與零售業皆被歸為服務業，是以國際貿易業應屬服務業之下，貿易商為服務之提供者[11]。

我國貿易商多為中小型貿易商，其貿易實績占全國整體貿易實績的一小部分。依我國中小企業發展條例之中小企業認定標準第 2 條，服務業的中小企業係「依法辦理公司登記或商業登記，並合於下列基準之事業：...前一年營業額在新台幣一億元以下者。」因欠缺我國貿易商之營業額統計資料，故參考貿易商過去三年的貿易實績，蓋貿易實績為貿易商通關時提供海關之資料，與貿易業者出進口貨物實付價格相關，應可部分反映出貿易商的營業狀況與收入。

依 2008 年至 2010 年國貿局資料，我國多數貿易商之貿易實績集中在四百萬美元以下，且分布在這個額度下的貿易商家數皆超過全體之 90%（表 1），反映出我國貿易商多為中小企業，特色為經營模式可能較為靈活，並會透過學習與經驗累積，快速地因應環境變化。然而，因廠商規模普遍較小，貿易商較不易掌握

[7] 同前註，頁 20。
[8] 同前註，頁 19。
[9] 張錦源、康蕙芬，國際貿易實務，頁 27，2006 年 10 月 6 版。
[10] 行政院主計處，中華民國行業標準分類第 7 次修訂（2001 年 1 月），中華民國統計資訊網，網址：http://www.dgbas.gov.tw/ct.asp?xItem=2203&ctNode=3374 （最後瀏覽日期：2011 年 6 月 20 日）。
[11] 行政院主計處，中華民國台灣地區國民所得統計摘要，中華民國統計資訊網，網址：http://www.stat.gov.tw/ct.asp?xItem=15060&ctNode=3536（最後瀏覽日期：2011 年 6 月 29 日）。

經營資源，加上其研發能力普遍薄弱、資金有限，故面臨較大的升級轉型困難[12]。有關貿易商的員工人數統計，依台北市進出口同業公會「2007 年貿易業經營環境調查報告」中 600 個統計樣本，專職貿易業務之專業貿易商占 67.3%，員工人數低於 50 人之廠商占 83.3%，顯示出貿易商內部人員偏精簡，無太多人力自行架設或維護電子商務相關設備[13]。

[12] 台灣綜合研究院，中小企業基本知識，台灣綜合研究院，網址：http://www.tri.org.tw/ceo/ （最後瀏覽日期：2011 年 6 月 29 日）。
[13] 台北市進出口商業同業公會，「2007 年貿易業經營環境調查報告」，頁 5-6，2007 年。

表 1　我國 2008 年-2010 年出進口廠商貿易實績分佈

單位：百萬美元

實績級距	2010 年廠商家數	2009 年廠商家數	2008 年廠商家數
未滿 1 百萬美元	87,155	86,709	85,724
1~2 百萬美元	8,450	7,600	8,301
2~3 百萬美元	3,838	3,211	3,735
3~4 百萬美元	2,166	1,796	2,169
4~5 百萬美元	1,419	1,157	1,443
5~7.5 百萬美元	2,043	1,670	2,008
7.5~10 百萬美元	1,076	916	1,077
10~20 百萬美元	1,898	1,465	1,850
20~30 百萬美元	632	469	631
30~40 百萬美元	354	270	357
40~50 百萬美元	214	173	215
50~100 百萬美元	479	350	455
100~300 百萬美元	368	287	344
300~500 百萬美元	79	60	65
500~1000 百萬美元	59	55	62
1000~5000 百萬美元	60	28	44
5000 百萬美元	8	6	9
總計家數	110,298	106,222	108,489

資料來源：經濟部國際貿易局

（三） 國際貿易活動

國際貿易中的每筆交易皆涉及繁瑣的手續，且因商品、付款方式、貿易條件與外匯貿易管制措施等不同，有不同的處理手續。以出口商之信用狀付款方式、CIF 為貿易條件為例，本小節大致將貿易流程區分為五大階段(圖 2)，分別如下：

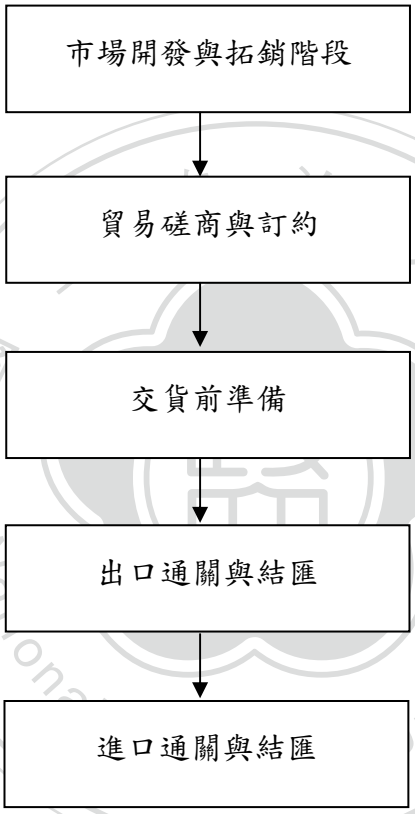

圖 2　國際貿易流程階段圖
資料來源：本研究製作。

1. 市場開發與拓銷階段

在市場開發階段，貿易商對市場進行了解與評估，並且搜尋貨源，在搜集資料後，開始擬定行銷相關策略、透過各種管道進行市場拓銷，藉由市場拓銷尋找交易對手，並且針對該交易對手進行徵信調查[14]。這些活動主要涉及資訊之搜集、

[14] 蔡孟佳，前揭註 3，頁 21-23。

分析、流通與散播，譬如市場調查，貿易商應注意政府機構出版、以及《台灣進出口月刊》、《貿易商刊》等刊物，以獲得最新市場訊息；貿易拓銷階段，貿易商可能以參展、網際網路、同業工會引薦等方式尋找交易對手；徵信調查時，貿易商可能透過對方所在的外國銀行、貿易商本國之銀行、徵信調查機構、駐外單位、其他客戶或對方國家商會，搜集該交易對手的資料，以判斷其信用情況[15]。

2. 貿易磋商與訂約

當貿易商找到交易對手、完成徵信調查、並且決定與其建立交易關係後，貿易商以函電、傳真等方式向對方為出口報價或進口詢價，雙方再就價格、產品品質、交貨、付款方式等事項為還價，直至雙方意思表示一致，交易即算成立。為降低日後產生爭議或糾紛的發生機率，貿易商通常會擬訂書面的進出口貿易契約（Import-Export Contract），在上頭載明所約定的交易事項與細節，或由一方就雙方口頭約定，製作交易確認書（Sales Confirmation；Purchase Confirmation），再由雙方簽字後各保留一份[16]。

3. 交貨前準備

建立交易關係後、出口商準備貨物前的這段時間，貿易商完成信用狀之開發與收受。一般而言，進口商先完成取得進口簽證、申請開發信用狀等手續，再委託銀行代轉信用狀給出口商，經出口商審核並接受後，出口商開始依情況申請出口簽證、辦理出口融資、準備貨物、洽訂艙位、依情況為貨物檢驗。又，依 CIF 條件，貨物越過出口港船舷後，運送風險由買方承擔，而賣方需為該貨物運送途中的滅失或毀損訂立保險契約、支付保費，是以本例的出口商亦須購買保險[17]。

完成上述事項後，出口商將貨物送往碼頭倉庫或貨物集散地，取得相關文件，以供出口報關。

---

[15] 同前註，頁 39-49；頁 60-62。
[16] 同前註，頁 23-24。
[17] 同前註，頁 25-28。

4. 出口通關與結匯

有關出口通關階段，出口商為求順利將貨物裝船出口，需在洽定的船舶結關前向海關申報通關，取得海關允許後提貨裝船。出口商先將貨物送進倉棧，進行報關作業，包含填寫報報單、檢附相關文件給海關、配合海關作業。海關決定予以貨物放行後，出口商持海關蓋印的出口報單至倉棧提貨裝船。裝船後，船公司與出口商分派人員檢查貨物件數與包裝情況，雙方理貨人員在理貨單上簽字、負責裝載的船上大副根據理貨單簽發大副收貨單（Mate's Receipt），出口商再憑大副收貨單向船公司換領提單（Bill of Lading，我國海商法稱之為「載貨證券」）[18]。

在出口結匯階段，出口商取得提單後應支付運費、並通知進口商裝運事宜，接著開製發票、根據信用狀條款規定準備有關文件，譬如匯票、公證報告、產地證明書等，待備齊所有規定文件或證明，則向信用狀指定的銀行提交信用狀及各種單據，押匯銀行審查所有單據、確認無訛後，即受理押匯、支付貨款給出口商[19]。押匯銀行接著將押匯的信用狀與押匯文件寄給開狀銀行，開狀銀行審查文件是否與信用狀完全相同，若其完全符合，開狀銀行一方面履行信用狀承諾，對押匯銀行進行補償，另方面則通知進口商進行結匯付款贖單[20]。

5. 進口結匯、進口通關與提貨

進口商收到開狀銀行的通知後，與銀行結清款項，取得出口商提示的押匯文件，便開始辦理進口通關與提貨之工作。進口商收到到貨通知後，持已取得的提單向船公司換領提貨單（Delivery Order），再持提貨單、發票、包裝單、輸入許可證或其他相關要求之文件向海關辦理進口通關，待查驗、繳稅後，持蓋印的提貨單到倉庫繳清倉租與相關費用，提領貨物[21]。貿易流程至此約告一段落，除非有索賠情事，否則出進口商從事貿易的目的於焉完成。

---

[18] 同前註，頁 28-29。
[19] 同前註，頁 28-31。
[20] 同前註，頁 31。
[21] 同前註，頁 32-33。

透過檢視貿易流程，可發現國際貿易之幾項特點。第一、國際貿易的主體雖然是貿易商，但還包含許多參與者，譬如徵信公司、開狀銀行、押匯銀行、物流業者、海關、報關行、保險公司。第二、國際貿易涉及許多文件填寫、傳送、核對、歸檔等，依我國財政部關稅局統計，2010 年全年度關稅局處理的進口報單共計 13,582,863 份，出口報單共計 10,269,780 份[22]。除了需提交給海關的企業與政府間（Business to Government, B2G）文件，企業彼此亦須準備企業之間流通的文件（Business to Business, B2B），譬如貿易商須製作報價單、訂單、購貨確認書、售貨確認書、買賣契約、匯票、商業發票、包裝單、重量尺碼單等，貿易商以外之人則需製作運送單據、保險單、檢驗證明書、產地證明書等[23]。第三、國際貿易涉及許多單據交易，譬如押匯銀行與開狀銀行皆依單據審核之結果決定是否放款，若相關文件沒問題，則銀行支付款項，是以單據的正確性至關重要。

貿易流程涉及許多文件處理與儲存，衍生出的問題為資料保存不易、資料傳輸不易，以及資料的正確性不易維持。若貿易單據皆為紙本，將對貿易商、報關行、政府及相關業者造成極大負擔；資料傳輸不易，係指資料在紙本或不同的電子文件格式，該些文件雖然部分內容相同，但不容易被直接複製、轉檔、傳送，將資料填載或輸入不同文件時，也難免造成錯誤。在全球自由貿易活動活絡之今日，貿易單據之流通數量亦將隨此潮流而增加，光是我國一年內之貿易單據，2010 年進口報單數量比 2009 年時增加 20.31%，出口報單數量則多增加 13.27%[24]。

二、 貿易業導入電子商務

近年來，電子商務（electronic-commerce, e-commerce）因其特性與外在環境

[22] 財政部關稅總局，財政部關稅總局發布 99 年第 4 季與 99 年全年度各項業務統計資料，財政部關稅總局，網址：http://web.customs.gov.tw/ct.asp?xItem=50595&ctNode=12661 （最後瀏覽日期：2011 年 7 月 1 日）。

[23] 張錦源，國際貿易實務詳論，頁 533，2009 年 8 月 14 版。

[24] 同前註 24。

需求，成為未來交易趨勢。電子商務使交易當事人得以透過電子與網路等形式，而非借助紙本文件的交易活動，加速交易活動進行。對貿易商而言，若廣泛應用電子商務，可使其提升交易效率，加速國際貿易腳步[25]。各國貿易商與企業早已運用不同類型的電子商務模式，譬如提供整合金流、貿易流的 Bolero、香港貿易通（Tradelink）、澳洲 Tradegate 等，皆是貿易活動導入電子商務的例子。在我國，政府與貿易商展開導入電子商務的具體內容，則包含提供國際貿易商品目錄及產業相關資料的入口網站，以及提供通關資訊存取與交換的平台。有關通關資訊之存取與交換，我國經濟部國際貿易局，展開「貿易便捷化計畫」，致力於通關無紙化與電子化，譬如制訂各機關簽審、檢驗、檢疫等文件的標準訊息，同時架設便捷貿 e 網，使貿易活動之整合更全面。

（一） 電子商務定義與範圍

電子商務泛指經由電子化形式所進行的商業交易活動。依經濟部商業司出版之《2010 中華民國電子商務年鑑》，將電子商務定義為「運用先進資訊科技，同時藉由組織作業的流程改造，來達到減低組織營運的成本開支，提升作業效率，增加客戶滿意度之商業活動[26]。」狹義的電子商務探討以數位化方式在網際網路上進行商業交易活動，廣義的電子商務則是指資訊科技通訊相關設備與應用如何提升商業交易活動價值，譬如商業、金融之電子資料交換（electronic data interchange, EDI）、網路下單、電子購物等，皆涵蓋在電子商務範疇[27]。

（二） 貿易業導入電子商務之概況

雲端運算蓬勃前，國際間的貿易活動中已存在許多利用電子商務之例子，譬

[25] 同前註，頁 16。
[26] 經濟部商業司，2010 中華民國電子商務年鑑，頁 1。
[27] 同前註。

如 Bolero 訂定標準傳輸格式，建置平台與資料庫，以供企業與金融機構交流，香港 Tradelink 和澳洲 Tradenet，提供各種處理電子文建的軟體與線上服務[28]。

我國貿易之電子商務發展，大致上為運用網際網路與書面之電子化，以提升貿易效率。依各種貿易商在各貿易流程的互動對象，可將貿易業導入電子化的模式分為 B2B 與 B2G。在 B2B 模式，貿易商利用網路平台、資料庫、軟體、EDI 等為各種溝通、製作文件、拓展貿易、維繫顧客關係；在 B2G 模式，則有我國政府推動「貿易便捷化計畫」，以簡化及調和國際貿易程序，並且利用電子方式達到無紙化貿易，以此大幅縮短貿易流程、降低貨物流動的成本[29]。

我國貿易便捷化計畫之進度停留在處理 B2G 文件。國貿局與相關政府機關已制訂各類 B2G 文件之標準訊息，並且建置供簽審、通關用途的「便捷貿 e 網」，貿易商或相關業者可將透過該等平台，文件單一輸入、重覆使用，以提升報關、簽審、檢驗、檢疫等流程的效率[30]。有關 B2B 文件，貿易商通常仍使用其所方便之形式為之，而無統一的文件[31]。

第二節　雲端運算之介紹與貿易雲端之導入

近年來，雲端運算開始受到企業與各國政府之重視。雲端運算的功能與特性為大型企業與中小型企業帶來不同好處，對大型企業，雲端運算可依需求隨時擴充或減少的彈性，可使其降低成本，對中小型企業，雲端運算提供各種簡便的服務，使中小型企業不用投入大量建置與基礎建設成本，即可透過網際網路使用應用程式與平台，甚至發展自己的網站及應用程式。

---

[28] Bolero, http://www.bolero.net/en/home.aspx (last visited Sept. 18, 2011)；Tradelink, http://www.tradelink.com.hk/chi/index.html (last visited Sept. 18, 2011)；Tradegate, http://www.tradegate.org.au/products/ (last visited Sept. 18, 2011).

[29] 經濟部國際貿易局，貿易便捷化簡介，網址：http://cweb.trade.gov.tw/kmi.asp?xdurl=kmif.asp&cat=CAT605（最後瀏覽日期：2011 年 7 月 7 日）。

[30] 經濟部國際貿易局電子商務小組，貿易便捷化計畫執行成效與展望，2010 年 11 月 5 日。

[31] 關貿網路，作者訪談內容。

雲端運算並非有利無弊，而其最受質疑的風險之一為資訊安全風險。雲端運算一大特色為透過虛擬化，以多租戶架構（multi-tenant）模式儲存不同企業或使用者的資訊，換言之，不同企業的資料將被儲存在同一硬體設備上，此舉引發資訊安全的疑慮，並且影響企業對導入貿易雲端之決策。

本節介紹雲端運算特性與概念，並且以貿易商需求為出發，以設定本研究之貿易雲端服務範圍和模式。

一、 雲端運算之概念、意義與特性

雲端運算的定義隨使用者的角度不同而有差異，加上雲端運算幾乎能套用在各種不同個人、企業、政府等的資料管理、處理、儲存，不同使用者對雲端運算的期待亦不相同。在討論貿易雲端適合的模式之前，宜先瞭解雲端運算的主要概念。以下分別介紹雲端運算概念、論者對雲端運算的不同描述與定義，包含美國國家標準與技術局（National Institute of Standards and Technology, NIST）於 2011 年發布的雲端運算定義與特性。

（一） 雲端運算之概念

雲端運算的概念是將電腦與網路處理資料的過程化繁為簡，申言之，雲端運算隱藏運算系統的複雜性，使用者不需理會資源的系統架構，也不需要太多專業技能，即可使用雲端運算資源來處理資訊。依字面解釋，雲端運算中所謂之「雲端」，指的是一群硬體和軟體的組合，譬如數據中心機房和一堆應用程式[32]。雲端運算的服務種類包含電子郵件、伺服器運算、資料儲存、資料傳輸、應用軟體與內容、系統服務等，提供這些服務的則是分散式運算，故資源雖四散在不同地

[32] Michael Armbrust et al, *A View of Cloud Computing*, Communications of the ACM Vol. 53 No.4 51, 52 (2010).

方，使用者卻可透過網路取得它們，同時使用者不一定知道、也不需知道從何、如何取得這些資訊[33]。

（二） 雲端運算的意義特性

雲端運算尚未有統一定義，而美國國家標準與技術局（National Institute of Standards and Technology, NIST）於 2011 年發布之「NIST 雲端運算定義草案（The NIST Definition of Cloud Computing (Draft)）」，當中就雲端運算目前發展情況為一描述與總結。依 NIST 草案內容，雲端運算係指使用者可隨時隨地、便利且按其所需地取得運算資源，那些資源皆來自於運算資源集合平台，包含網路、伺服器、儲存功能、應用程式與服務。運算資源可以被重新配置，且在被提供給使用者時，是以快速、最低管理程度及與服務提供者最少交流互動的方式為之[34]。

NIST 指出，雲端運算除符合上述描述之外，還具有五項重要的特性，分別為使用者可自助式地依需求取用（on-demand self-service）、廣泛的取得管道（broad network access）、使用者共享資源池（resource pooling）、快速部署之彈性（rapid elasticity）與量測服務之功能（measured service），相關說明分述如下[35]：

1. 自助式地依需求取用

使用者可以在不與服務提供者接觸的狀況下，單方取用所需要的資源、或為資訊之儲存[36]。

---

[33] 拓墣產業研究所，探索雲端運算市場新商機，頁 12-13，2010 年 7 月。
[34] Peter Mell & Timothy Grance, *The NIST Definition Of Cloud Computing (Draft)*, NIST Special Publication 800-145, 2 (Jan., 2011). *available at* http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf (last visited July 10, 2011).
[35] *Id*.
[36] *Id*.

2. 廣泛的取得管道

使用者可透過不同類型的載具取得雲端運算服務[37]。

3. 使用者共享資源池

服務提供者透過多租戶架構聚集資源，供不同使用者使用。使用者通常不知道資源的確切來源，亦無法控制資源被存放的位置，然而使用者可大略掌握資源被存放在哪個國家、哪個數據中心[38]。

4. 快速部署之彈性

雲端運算可在極短時間內依需求調節產能，且在某些雲端運算，這項功能已交由自動化執行。對使用者而言，這個特性代表對雲端運算資源的取之不盡，隨時可購買得到[39]。

5. 服務被監控與量測

因雲端運算服務的計價方式採「付費多少、使用多少」的模式，加上取得服務過程中，使用者與服務提供者之間通常沒有太多交流，故系統中設有計算工具，可監管、掌控、回報各種服務被使用的時間、程度與使用情況，以提升雙方在交易過程中的透明度[40]。

前述原因之外，雲端運算服務之量測，可幫助使用者知悉其使用量與須支出的費用，以較有效率地計算導入雲端運算的成本，藉此規劃財務。

二、 雲端運算態樣

雲端運算態樣普遍被以兩種方式區分。依雲端運算之服務提供內容，可被分

[37] *Id*.
[38] *Id*.
[39] *Id*.
[40] *Id*.

為「軟體即服務」、「平台即服務」、「基礎設施即服務」，若判斷該雲端運算服務之開放性，則可分為「私有雲端」、「公用雲端」、「社群雲端」及「混合雲端」。

（一） 依服務提供內容區分

雲端運算服務提供類型被區分為三種，分別如下：

1. 軟體即服務（Software as a Service, SaaS）

SaaS 係指服務提供者將軟體儲存在某個遠端伺服器上，透過網路，使用者得以遠距離地使用該軟體。SaaS 服務內容型態與傳統軟體購買相似，差別在於過去軟體被當成「產品」購買，使用者經過授權後，下載、安裝軟體於個人電腦上，而 SaaS 是將軟體視為「服務」，由使用者在網路上取得並使用[41]。

對企業而言，SaaS 最大的好處為減少對基礎建設的投入成本。多數情況下，一般瀏覽器即可支援 SaaS 的軟體，且維護、升級之工作皆由服務提供者負責，企業不需費太多資源在資訊設施，並可獲得最新、最有效率的資訊處理工具[42]。

2. 平台即服務（Platform as a Service, PaaS）

在 PaaS 服務模式，服務提供者提供虛擬平台，使用者可在該平台上發展自行設計的應用程式或服務，並且透過該平台將程式提供給其他人[43]。使用者的應用程式只要符合該平台要求的程式語法（例如 Java、python、.Net），即可將該應用程式放在平台上。

企業導入 PaaS 的好處，主要為以較低成本自行開發平台。在過去，企

[41] TIM MATHER et al., CLOUD SECURITY AND PRIVACY 17-18 (2009).
[42] *Id*.
[43] *Id*., at 19.

業若要架設網站、或設計應用程式，通常需具備許多與架設網站相關或製作軟體的專業知識，並且添購伺服器及相關硬體設備，若改導入 PaaS 模式的服務，企業架設網站或開發軟體所需要的硬體、軟體及知識，則皆由服務提供者負責或幫忙分擔，使得自行開發變得較可行，也較不費力[44]。

3. 基礎設施即服務（Infrastructure as a Service, IaaS）

IaaS 服務模式係服務提供者提供基礎設施服務。IaaS 服務提供者提供的服務是資料處理與儲存的空間與設施，且可令使用者依其所使用的量決定付費額度，進而令使用者擁有調整產能的彈性與空間[45]。IaaS 服務的提供方式類似於公用運算（utility computing），公用運算係企業透過租用模式，將資訊儲存與運算服務視為水、電相同的公用服務，企業可依其所需的量為租用，且不需自行管理設備，與 IaaS 模式下使用多少基礎設施付費多少，且使用者不管理基礎建設、資訊放置地點乙節相似[46]。

（二） 依雲端服務之開放性區分

依雲端之開放性，其可被區分為私有雲端、公有雲端、社群雲端及混合雲端。對企業而言，採取哪種雲端運算模式，代表著企業內部與網際網路之間的關係呈現何種程度的關聯性，以及企業使用該雲端運算的能力、範圍、規模、虛擬化資源及網際網路連結度[47]。在以下四類之中，私有雲與公有雲亦分別被稱為「內部的雲端運算（internal）」與「外部的雲端運算（external）」，這些名稱更可體現出企業對網際網路的開放程度[48]。

---

[44] *Id*., at 19-21.
[45] *Id*., at 22.
[46] Wikipedia, Utility Computing, at http://en.wikipedia.org/wiki/Utility_computing (last visited Jul. 10, 2011); TIM MATHER et al., *supra* note 41, at 22.
[47] TIM MATHER et al., *supra* note 41, at 32.
[48] *Id*.

1. 私有雲端（private cloud）

私有雲端是只供某一機構或企業使用的雲端運算。私有雲端的使用者不用跟他人共用，故企業多自行維護、或請第三人維護該雲端運算。因使用者只有一個機構或企業，論者有認為該數據中心的大小有一定之規模，否則該等設備僅稱得上是一般的中小型數據中心，就算該數據中心採用虛擬化技術，也難被視為雲端運算[49]。導入私有雲的好處在於較不用擔心雲端運算的資訊安全問題，雲端運算是否與公司治理的目標相符，或者其他雲端運算的困難。私有雲端的缺點在於無法使企業達到降低成本的目的，蓋管理或維護該雲端運算的成本仍僅由一公司或機關負擔[50]。

2. 公用雲端（public cloud）

公用雲端係指以一雲端設施供給不同使用者使用。公用雲端的資源通常由多人共享，由一個或數個服務提供者提供設施與資源。公用雲端由服務提供者掌握，並且負責維護設施、確保資訊安全風險不要發生，使用者則無太多控制權限[51]。

3. 社群雲端（community cloud）

社群雲端係供給數個機關使用的雲端運算，其開放程度介於私有雲端與公用雲端之間。社群雲端通常係供給數個有共通目的、需要分享相同資訊的機關，並且由這些機關或委託第三人提供與維護該雲端[52]。在某些論述的分類之中，不一定將社群雲端設為一項分類。

---

[49] Michael Armbrust et al, *supra* note 32, at 52.
[50] TIM MATHER et al., *supra* note 41, at 23.
[51] *Id*., at 23.
[52] Peter Mell & Timothy Grance, *supra* note 34, at 3.

4. 混合雲端（hybrid cloud）

混合雲端係由兩個以上的雲端組成，分別為私有雲端與公用雲端，二者之間設有連接機制，可供資料移轉。企業若採用混合雲，可將不具機密性的資訊分配在公用雲端處理，將具機密性的資訊保留在私有雲端[53]。

雲端運算內部的層次，大致上可以堆疊的概念想像（圖 3）。在服務使用者一方，服務使用者透過電腦和瀏覽器，對雲端運算不同層級取得服務。在 SaaS 模式與 PaaS 模式中，雲端服務主要內容皆是虛擬化的資源，包含應用程式和平台，IaaS 模式在雲端運算整體之最底端，主要為存放資源的硬體設施。

[53] TIM MATHER et al., *supra* note 41, at 25.

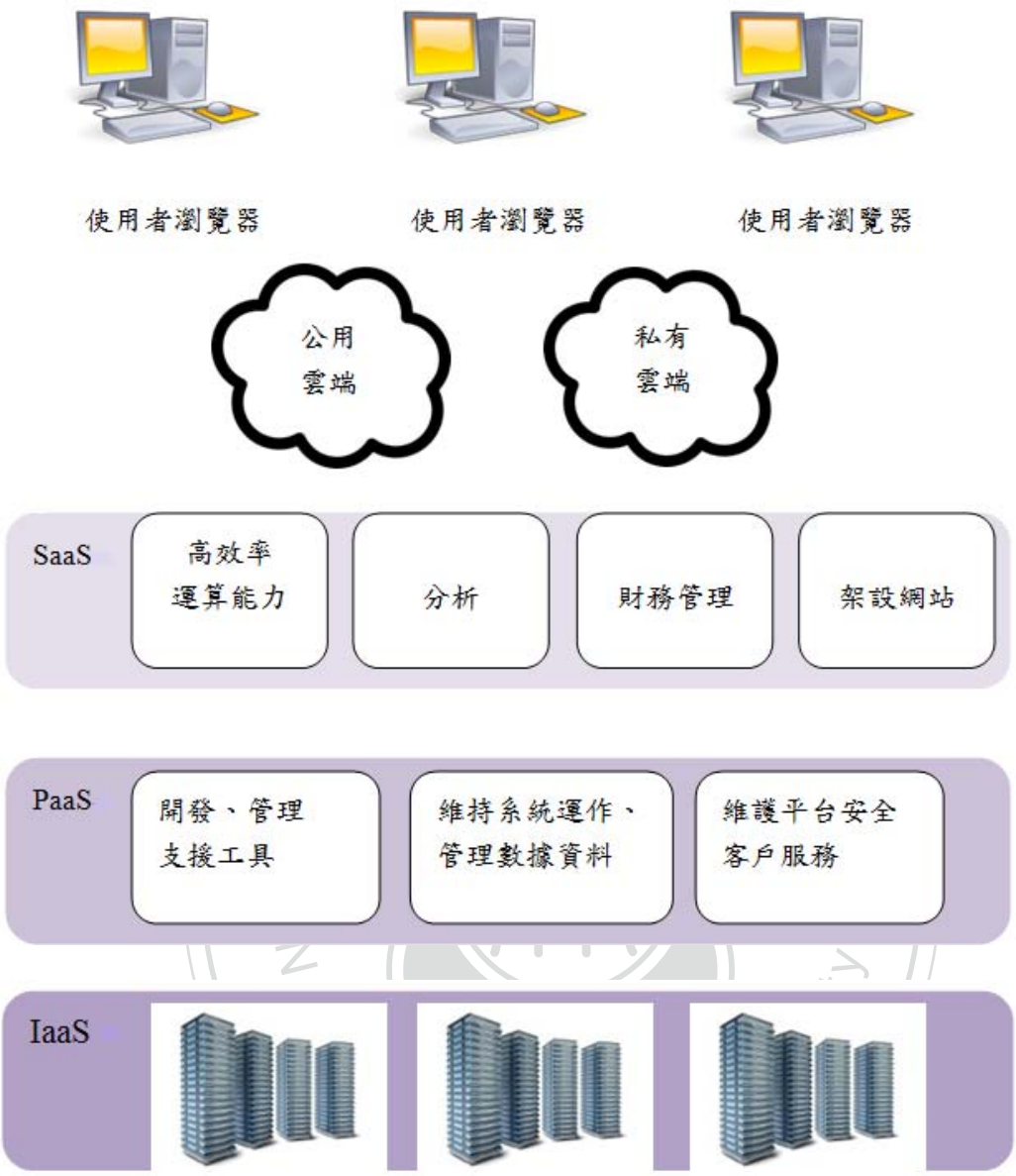

圖 3　雲端運算架構示意圖

資料來源：本研究製作。

三、 雲端運算與傳統模式比較

雲端運算與傳統模式的比較結果，影響企業是否導入、以及如何導入雲端運算等事項。若二者之間沒有差異、或相異之處無足輕重，則已導入電子商務、或設立資訊科技（Information technology, IT）部門的企業，似乎沒有導入雲端運算的必要；對於尚未建置 IT 部門的企業，若其決定導入雲端運算，則這些企業的導入方式或可直接借鏡過往的模式，不須特別考慮是否導入雲端運算。

依傳統模式，提供的服務有硬體、軟體、全球資訊網、電子郵件、檔案傳輸、遠端登入、新聞討論區、電子佈告欄等。在既有的電子商務模式中，企業多將硬體放在公司內部、或委託人代為管理，軟體則購買、取得授權後，將其安裝在公司硬體上使用。全球資訊網、電子郵件、檔案傳輸、遠端登入、新聞討論區及電子佈告欄，則是網路服務的一部分，具有傳輸資料、取得資料等功能[54]。

電腦網路傳遞資訊的模式，若依伺服器與客戶端之關係分類，可分為伺服器型網路（server-based）與對等型網路（peer-to-peer）。在伺服器型網路的情況，網路內眾多客戶電腦端分別向伺服端提出需求，伺服端會依個別客戶的需求給予回應（圖 4）；在對等型網路的情況，每台電腦同時扮演伺服端與客戶端角色，可提供資訊、亦可向其他電腦提出需求。相對於伺服器型網路，對等型網路之建置成本較低，但管理較麻煩（圖 5）[55]。大多數網路系統會結合這兩種網路類型[56]。

[54] 高大宇等人，資訊安全，2003 年，頁 40-42。
[55] 同前註，頁 32-25。
[56] 同前註。

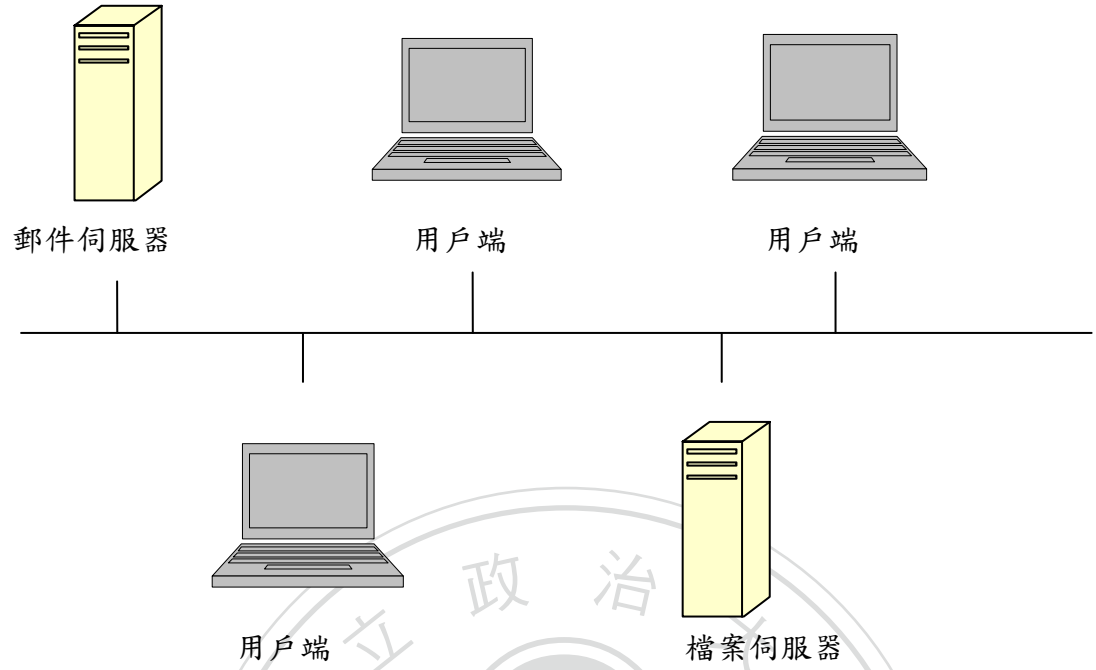

圖 4　伺服器型網路

資料來源：高大宇等人，資訊安全，2003 年，頁 34。

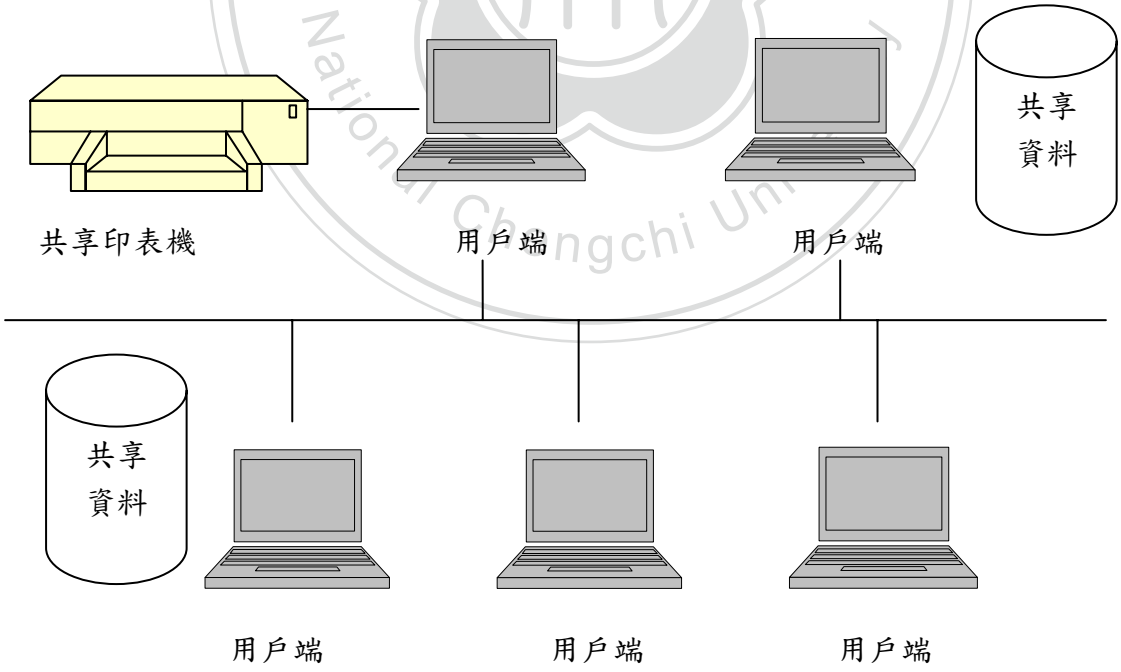

圖 5　對等型網路

資料來源：高大宇等人，資訊安全，2003 年，頁 32。

傳統模式與雲端運算皆是一系列硬體與軟體的組合，且都涉及網際網路之使用，其中不同的地方，大致包含下列幾點：

（一） 購買與付費方式不同

傳統模式將電腦與網路視為「產品」，雙方以買賣形式交易，買方一次投入建置硬體的資本，預付軟體授權費用；雲端運算將電腦與網路視為「服務」，採付費後使用、使用多少付費多少的計價方式。

（二） 軟體維修、升級與更改之負責方不同

傳統模式中，雙方就產品採一次買斷，某些供應商會提供保固期限，保固期限過後，若企業欲維修或升級軟體，須另外締結維護契約或其他類型契約，是以軟體相關的維護措施，多由企業負擔；雲端運算情況下，雲端服務提供者多負有提供最新的服務內容，並且負擔軟體維修、維護與升級的義務，企業不需自行維護軟體。

（三） 資訊與軟體存放地點不同

在傳統模式中，資訊與軟體存放地點為企業的主機，由企業管理與掌握；在雲端運算下，資訊與軟體被放置在遠端的平台上，由服務提供者維護與持有，企業透過網際網路取用其所需資訊和軟體資源。

（四） 平台的使用者數量

傳統模式的網路平台擁有者為企業，並無他人共用；在雲端運算模式中，不同使用者在同一平台上活動，遵守雲端服務提供者設下的規範，並依照該平台要求的程式語法和支援軟體從事應用程式開發或網站建置。

（五） 平台的擴展性

傳統模式中，使用者在管理時不用考量平台的擴展性；在雲端運算模式中，因平台使用者不只一人，雲端服務提供者須考慮平台擴展性問題，以在不同流量時皆有效管理平台活動。

（六） 平台管理方式

傳統模式中，平台由企業管理，企業多透過內部 IT 人員或委託第三人管理網路平台；在雲端運算模式中，雲端服務提供者同時將同一平台提供給許多人使用，因此採行整合式管理（integrated management），並且在平台上設立監管與計算不同使用者之使用量等系統，以便其管理。

（七） 基礎建設之取得

傳統模式中，企業多購買或租用基礎設施，且需求量增加時，因採購的單位多為一台、一座機器，容易添購多餘設備；在雲端運算模式，企業依其所需的使用量採購基礎設施，並且以使用量計價，較不會碰到採購過剩的問題。

（八） 設備存放與管理

傳統模式中，基礎建設的存放地點與管理皆由企業自行負擔；在雲端運算模式，基礎建設存放在雲端運算服務提供者的機房，並由雲端服務提供者負責管理，企業不須額外付出空間或多於 IT 人力。

由上可知，傳統模式在交易時將 IT 設備視為產品，其付費與建置的金額及規模較缺乏彈性，同時，企業須負擔大部分維護及保管資訊的責任，整體網路資訊呈現較分散的狀態。在雲端運算模式中，企業的資訊與資源皆被放置在遠端的平台上，企業僅需透過簡單的設備和網際網路，即可以服務模式取得剛好需要的資訊與資源，又，資訊與資源在網路環境的分布上，呈現較為集中的狀態。

四、 雲端運算對企業帶來之優點與障礙

由雲端運算的特性，以及雲端運算和傳統模式的比較，可觀察出雲端運算帶給企業的好處，有部分是傳統模式無法替代的，但導入雲端運算亦須面臨風險，這些風險可能造成企業對雲端運算裹足不前。本小節分別檢視雲端運算對企業帶來的優點與障礙。

（一） 雲端運算對企業帶來的優點

雲端運算對企業帶來的好處包含具備彈性、企業不需自行負擔軟體維護或硬體存放、服務提供者提供不同程度的現成服務、以使用量計算服務費用、方便資訊之管理與追蹤。以下分別敘述：

1. 服務具備彈性

雲端運算具高度擴展性，可在短時間內自動依需求調整產能，使得資源部署快速且適當地符合所需，較不易產生產能過剩或不足的問題。

2. 企業不需自行負擔軟體維護或硬體存放

雲端運算係以服務模式提供，其資源被存放在遠端的硬體設備上，由服務提供者負責管理。企業僅需透過瀏覽器等簡易設備即可取得最新之服務內容。對企業而言，不需自行負擔維護費用或存放空間，可為其節省 IT 成本，將資源投注在其他部門。

3. 服務提供者提供不同程度的現成服務

此一優點在PaaS模式中較為明顯。因服務提供者多採多租戶架構管理，

係以同一服務內容供給不同客戶，為求方便管理與維護平台，服務提供者多半發展出既有之規範、語法限制等，並且提供使用者支援軟體。

4. 以使用量計算服務費用，且導入時不須投入太多資本

在傳統模式下，企業若欲導入電子商務，付費模式通常為以產品為單位、一次購足、預付費用，因此初期時須投入較多之成本，在增建硬體設備時，不管新需求多寡，購買的硬體設備以一套為計算單位，導致每次擴增的資本開支較為僵固，且無法採購剛好符合其需求的數量。在雲端運算模式，計費依據是服務的使用量，企業每次導入可添購剛好符合需求的數量，使得企業不必在初期一下子投入大量成本，往後調整 IT 規模時，也不需為滿足部分需求而增購多餘的設備。相關舉例如表 2 所示。

表 2　自建客戶關係管理系統（CRM）與中華電信 CRM 服務價格差異表

項目	自建 CRM 系統	租用中華電信 CRM 系統
硬體設備購買	30 萬	0
軟體添購費用	15 萬	0
平台月租費	0	23 萬
IT 人力維運費用	48 萬	0
第一年總持有成本	93 萬	約 23 萬

資料來源：善用雲端，中小企業也能成就大事業，貿易雜誌 241 期，頁 18，2011 年 7 月。

5. 方便資訊之管理與追蹤

雲端運算因以使用量計費，加上多租戶架構管理，且具有自動化之特性，故服務提供者須建置完整之追蹤記錄，以使其管理上更容易、交易相關資訊更透明。

（二） 導入雲端運算的障礙

阻礙企業導入雲端運算的原因很多，以下歸納與雲端運算本身較相關者，分別為企業就服務本身、導入過程、對資訊之掌握程度與資訊安全問題等事項的顧慮，這些顧慮都將導致企業較不願意導入雲端運算[57]。企業對雲端運算應有的顧慮如下：

1. 及時取得需要的服務

雲端運算的背後由一群軟硬體支援，這些支援設施之所以無法被取得或使用，原因來自於停電，服務本身未準備就緒，服務提供者因其內部因素（譬如破產、併購）而停止服務提供，服務維修或升級時不能同時進行服務提供等不同事項[58]。

2. 中途轉換服務提供者

不同服務提供者之間的介面與應用程式不一定相容，且在PaaS模式下，各個提供平台的服務多自訂規範和系統規格要求，若其彼此不能互通，企業會擔心導入雲端運算之後，難以退出該雲端運算服務[59]。

3. 資料轉移到雲端上須耗費成本

企業若本身早有IT設備，將該些設備上的成果移轉到雲端運算上，將耗費許多成本及心力，使得企業寧願固守原有設施[60]。

---

[57] Roger Clarke, *User Requirements for Cloud Computing Architecture*, 2010 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing 625, 627(2010).
[58] *Id*.
[59] Michael Armbrust et al, *Above the Clouds: a Berkeley View of Cloud Computing*, Technical Report No. UCB/EECS-2009-28, University of California at Berkeley (2009).
[60] *Id*.

4. 預測雲端運算的效率

雲端運算本身的設計結構與上頭存在的系統將影響其運作速度，若雲端服務提供者致力於改善其設計，譬如消除雲端運算的某些疊層，即可提升整體系統作業的速度，進而使企業成本降低、效率提升[61]。

5. 修復過程將造成的影響

雲端運算多為一龐大系統，若當中有錯誤，其需具備該錯誤、以及除錯過程不影響雲端服務提供者提供其他服務[62]。

6. 雲端運算其他使用者對企業的影響

同一雲端運算服務下之所有企業、以及服務提供者，彼此在服務提供層面、法律責任等，皆可能相互影響，故當中一參與者不適當的行為，將影響其他方使用雲端運算，譬如一使用者被偵測出是惡意行為，其他系統遂阻斷同一伺服器下所有資訊交流，又或某一使用者需負擔法律責任，服務提供者通常不希望自己負擔連帶責任[63]。

7. 資料機密性及對資料的審計性

雲端運算服務提供者將資料放置在遠端集中的設備上，企業無法直接掌握其資料，加上目前雲端運算環境多偏向開放、資料可能被放在企業營業所在地以外的國家，因為每個國家的司法環境不同，該企業的資料不一定能毫無障礙地流通。考量這些事項，將使企業較不願意導入雲端運算[64]。

理論上，除了法規限制的影響較難消除之外，前述七點事項可透過技術達到

[61] *Id*.
[62] *Id*.
[63] *Id*.
[64] *Id*.

解決功效[65]。但因為企業本身對雲端運算不一定具被充分了解，企業仍可能在決定是否導入雲端運算時，產生上述疑慮。

五、 貿易雲端範圍與導入之模式

「貿易雲端」在我國並無一具體形式或範圍。就字面意義而言，可能為「貿易商之雲端運算」或「貿易活動之雲端運算」，若採前者解釋，貿易雲係指供貿易商使用的雲端運算，採後者解釋，則貿易雲係供貿易活動所使用，使用者除貿易商，尚包含其他參與貿易活動流程之企業與機構。依我國經濟部在 2010 年推動「雲端運算產業發展方案」下的貿易雲端服務，將貿易雲端的主要功能擺在貿易無紙化、電子化服務、創新貿易服務業，以求提升我國貿易競爭力，從其架構觀察，係採後者解釋。

經濟部國貿局雖就貿易雲端展開研究，並與貿易商及相關部會開會討論，提出一個貿易雲端服務架構（圖 6），然而此計畫目前已停止，近期內應不會有進一步發展。在業界，亦尚無貿易雲端運算平台。是以本研究參考貿易商特性、國際貿易活動、雲端運算性質與導入等事項，進而假設本研究討論之貿易雲端。

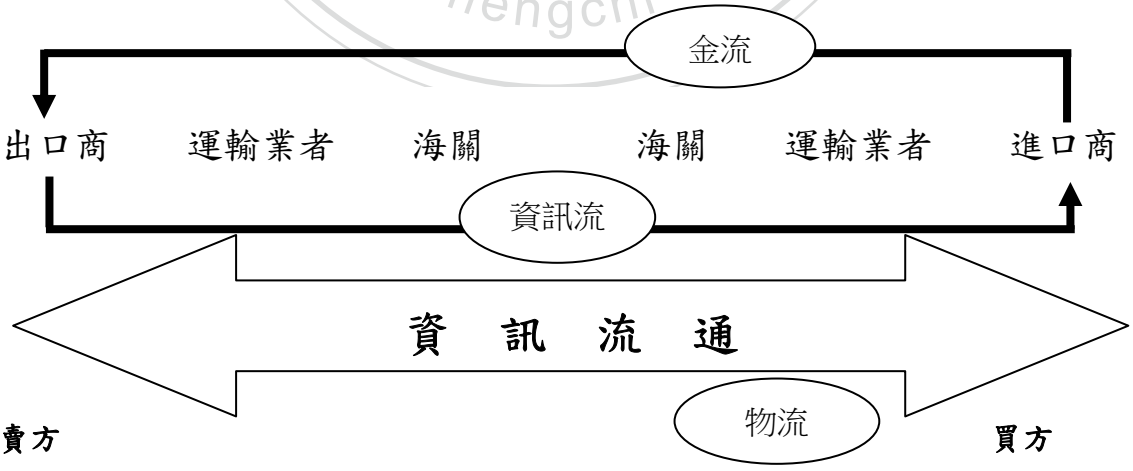

圖 6　國貿局貿易雲端服務示意圖

資料來源：經濟部國際貿易局。

[65] *Id.*

貿易雲端應支援國際貿易中的大部分活動。貿易雲端應盡可能納入貿易相關應用服務，理由包含：第一、貿易活動與一般商業活動有諸多不同，尤其在進出口流程中，貿易商與相關機構有許多文件交流，範圍涵蓋銀行、物流業者、報關行、海關及政府機關，文件繁多複雜、格式不一，這是一般商業活動或對消費者之電子商務所沒有的，是以貿易雲端之存在與特別設計有必要性。第二、因貿易活動中對各方資訊與文件交流之需求，貿易雲端應重視資源的流通性、以及與國際接軌，是以參與者數量與其活動之增加，將對貿易雲端帶來較多助益，進而促進其品質提升，若在設計時納入貿易商願意使用貿易雲之誘因，亦即使貿易雲端具備眾多支援功能，將可提升貿易商與相關業者加入的意願，進而吸引更多未導入貿易雲端的業者投入，使更多使用者分攤同一雲端運算系統之成本，同時達到彼此分享資源，以及貿易雲端主要設置之目的。有鑒於此，貿易雲端應納入貿易流程中商流、物流、金流、資訊流，使得貿易商的一般商業活動皆能透過貿易雲端服務進行。

個別貿易商在導入貿易雲端之前，應評估其是否適合導入，以及應如何導入。隨著外部環境為國際競爭日趨激烈，貿易活動電子化的趨勢，加上各產業「去中間化」，我國傳統貿易商之中介功能越來越衰退。考量我國專業貿易商多為中小企業，普遍缺乏雄厚資本與研發能力，導入貿易雲端，理論上可使貿易商以相對低廉的成本導入電子商務，該貿易雲端則可幫助貿易商帶來更多競爭優勢，包含提升效率、節省成本、開發加值服務。

依我國貿易商的特性與條件，最理想的貿易雲端服務導入模式為 SaaS 模式與 PaaS 模式，並採混合雲端模式。我國貿易商因人員精簡、研發能力與資源有限，性質上偏向剛起步使用電子商務的企業，若採 SaaS 模式與 PaaS 模式，可以取得較多現成的服務，不用自行開發或維護，並且因先前電子商務發展規模有限，在導入時較不易發生資料移轉不便、系統與雲端運算環境不相容之問題。有關導入貿易雲端之開放性，貿易商除許多貿易文件的資料不應被洩漏之外，貿易商之間的合作關係與相關電磁紀錄，亦應給予保護。是以在導入雲端的開放性上，貿

易商宜將其資料與相關服務區分為兩部分，較機密、供內部使用之資料歸入私有雲端，欲提供予公眾或其客戶者，則放置在公用雲端上。惟混合雲端構造兼具公用雲端與私有雲端，導入私有雲端會提高整體雲端運算導入的成本，對規模較小、預算較多限制的企業而言，或許較不具吸引力。

總結上述，本文認為較理想的貿易雲端運算模式如圖 7 與圖 8。

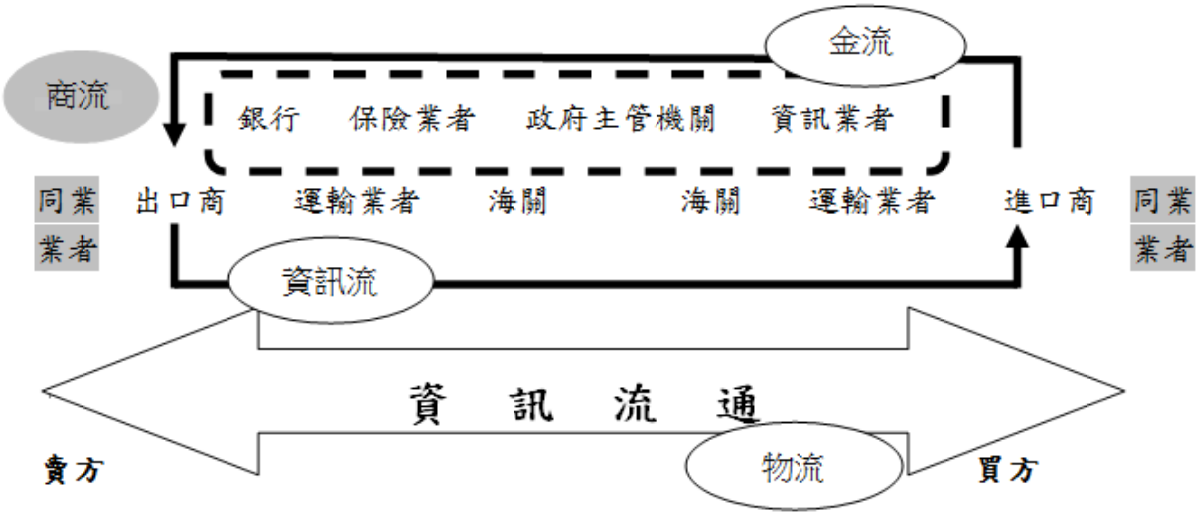

圖 7　本研究貿易雲端服務示意圖

資料來源：本研究製作。

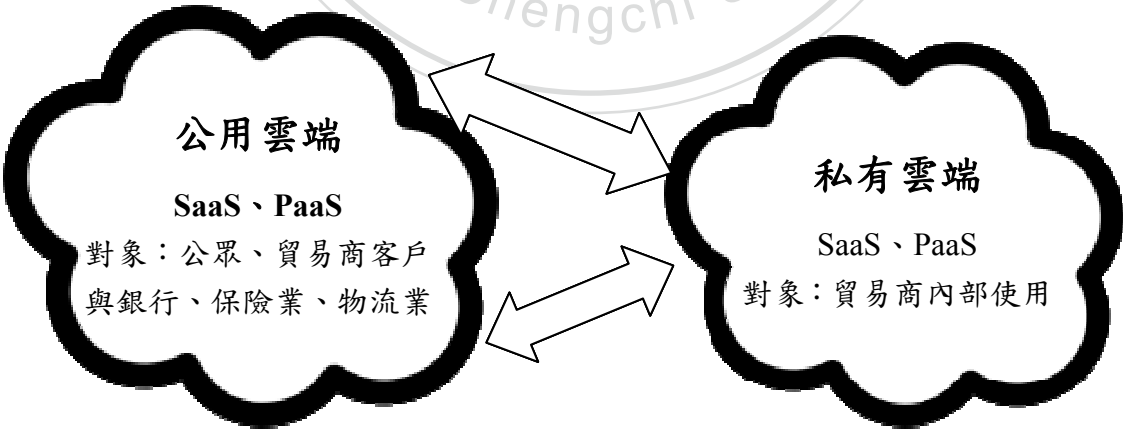

圖 8　本研究之貿易商導入貿易雲端示意圖

資料來源：本研究製作。

第三節　小結

我國貿易商面臨國際上之激烈競爭，加上廠商跨過中介商，直接向上游採購，是以造成貿易商競爭力流失。依我國貿易商之規模與狀況，導入雲端運算為主之電子商務係為一理想之模式。基於提升貿易商之效率與降低其成本，貿易雲端應該加入所有貿易流成中之作業服務與加值服務，以吸引更多廠商加入，擴大貿易雲端之可用性與降低其營運成本。就個別貿易商而言，因我國貿易商多為中小企業，故採 SaaS 模式與 PaaS 模式、並以混合雲端方式導入，可能使其不用專注於研發系統或維護系統，並且在開放性上有所彈性。

第三章、貿易雲端之資訊安全風險與資訊安全風險之控管

資訊安全是貿易商決定是否導入貿易雲端時的重要因素。貿易商扮演國際商業活動的中介角色，使各個國家的廠商得以互通有無，故其最大的資產與競爭優勢來自於對商機、貨源等資訊之掌握，若這些資訊未受到保護，將對貿易商帶來極大風險與損害。

因貿易雲端服務的概念是集中資源，再依貿易商所需，從雲端上取得適當的資訊與資源，故貿易商的資訊將透過網際網路處理、並很可能被存放在非自有的機房或設備上，導致貿易商對這些資訊的掌控程度降低。若貿易商不清楚其資訊的所在環境，或是資訊被存放在其他國家，受到該國政治、法律、網路環境等影響，將導致貿易商不易控制資訊，甚至不能隨時取得資訊，這些特點將貿易商在決策是否導入貿易雲端時，對貿易雲端的資訊安全產生疑慮。因此，確保貿易雲端的資訊安全，以降低貿易商的疑慮，應可提升貿易商導入貿易雲端的意願。

要降低貿易商對貿易雲端資訊安全的疑慮，須先找出貿易雲端資訊安全風險，進而對症下藥，以提升資訊在貿易雲端上的安全性。為求了解貿易雲端資訊安全風險，須認識何為資訊安全、資訊安全的標準、貿易雲端中存在哪些資訊安全威脅，進而提出消除或降低資訊安全威脅的方法。本研究將消除資訊安全威脅的辦法區分為管理、技術、法規三類，分別參考傳統模式、雲端安全聯盟（Cloud Security Alliance, CSA）之建議，以及我國目前的電子與網路資訊安全法制環境。

第一節　「資訊安全」相關介紹

「資訊安全（information security）」係指維護資訊，確保資訊不在未經授權

的情況之下被取得、使用、揭露、中斷、變更、毀損[66]。資訊安全之「資訊」，可能是電子數據，亦可能是書面、口語等不同方式呈現出來的內容[67]。本研究主要討論貿易雲端的資訊安全問題，故在此所指的「資訊」，係指電子化的內容，包含構成資訊的數據（data）、資訊、以及資訊集合成的知識（knowledge）[68]。

資訊安全的基本功能與目的，是保障資訊的保密性（Confidentiality）、完整性（Integrity）、可用性（Availability）、認證性（Authenticity）與不可否認性（Non-repudiation）[69]。「保密性」係指確保資訊傳輸或儲存時的私密性，使資訊不被未授權者取得或揭露；「完整性」係指資訊在任何階段不被不適當地修改或被毀損；「可用性」係指經授權的使用者可適時地取得並使用資訊；「認證性」係指主機（host）或服務能夠驗證使用者身分；「不可否認性」係指接收的一方不得否認其未接收訊息、傳輸的一方不得否認其未發送訊息[70]。（圖 9）

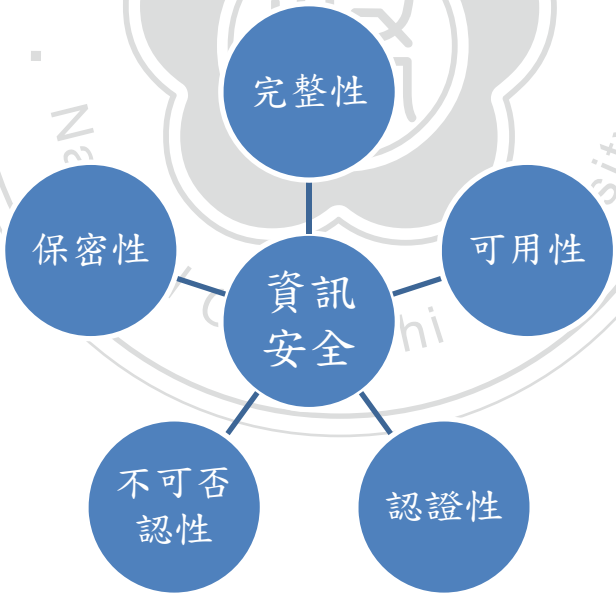

圖 9　電子化資訊的基本功能與目的

資料來源：本研究自製。

[66] Wikipedia, *Information Security*, WIKIPEDIA, *at* http://en.wikipedia.org/wiki/Information_security#Key_concepts (last visited Jul. 7, 2011).
[67] KRAG BROTBY, INFORMATION SECURITY GOVERNANCE 7 (2009).
[68] *Id*.
[69] *Id*., at 5-6.
[70] *Id*.

由資訊安全的五個基本功能與目的，可得知使用者及服務提供者的資訊安全管理，目的係為使被授權的人得以在被授權期間內取得正確的資訊。為求確認哪些使用者有權限、哪些使用者無權限，系統須有辨識使用者身分的功能。此外，在電子商務中，為使雙方無法否認其交易，系統須有某些簽署或類似的功能，使交易雙方在送出資訊、接收資訊與存取資訊時，無法否認其已做出的行為。

企業在導入雲端運算時，應進行風險評估，以及未來之風險管理策略。依國際標準化組織（International Organization for Standardization, ISO）下之「風險管理原理及指導綱要（Risk Management- Principles and Guidelines）」，「風險」係指目標結果的不確定性[71]。因服務提供者與企業無法確保雲端運算之安全性毫無漏洞，故企業導入雲端運算，將承受一定程度之資訊安全風險。又資訊安全風險之實現與否存在於未來，其結果與目前之間有時間之差距，在這段時間之內，人們可使用各種方式試圖控制風險之發生，這類活動為資訊安全之控管。

第二節　貿易商在貿易雲端的資訊安全風險

依貿易商的主要活動內容，貿易商較可能使用貿易雲端中的資訊儲存與資訊處理服務。貿易商主要工作重點為貿易拓銷、尋找商機、客戶及貨源、與客戶維持良好關係，貿易流程中的文件製作與檔案轉換則多由報關行或物流業者等參與者處理，是以貿易商使用的貿易雲端服務，應與資訊收集、分析、保存，以及即時更新客戶關係管理系統(customer relationship management, CRM)等活動相關，這些服務多具備資訊儲存及資訊處理功能，資訊儲存時須使用空間的服務，處理資訊、架設網站等工作，則涉及使用應用程式與平台等服務。通關、傳遞文件等工作，雖是貿易活動中的一環，但因多交由其他貿易相關業者處理，就貿易商而言，較不屬於其所使用的貿易雲端服務。

[71] ISO Risk Management- Principles and Guidelines (ISO 31000: 2009(E)), ISO, *available at* http://www.iso.org/iso/catalogue_detail?csnumber=43170 (last visited Jul. 19, 2011).

貿易商使用的貿易雲端服務範圍涵蓋三種服務模式。對中小型貿易商而言，較可能導入的貿易雲端是 SaaS 模式與 PaaS 模式服務，但這類服務模式涉及的資訊暫存與儲存，基本上是 IaaS 模式服務提供者提供給 SaaS 模式或 PaaS 模式服務提供者，再由這些模式的服務提供者提供予貿易商[72]。對大型貿易商而言，以其原有的資本與研發能力，導入 IaaS 模式亦不失為一理想模式，蓋在 IaaS 模式下，貿易商將較不受限於平台系統與語法，且較容易將已發展的其他 IT 資源移轉至雲端上。因三種服務模式對貿易商皆有影響，在討論資訊安全時，應將這三種模式共通與個別的資訊安全風險全納入考量。

一、 貿易雲端資訊儲存與資訊處理之特性

貿易雲端的資訊儲存地點，是導致資訊安全產生漏洞的一大因素。貿易雲端資訊儲存地點衍生下列疑慮：

1. 儲存地點不是貿易商的自有設備上，而是貿易雲端服務提供者的設備；
2. 儲存方式採行多租戶架構，各家資訊被集中儲存於同一硬體上，再透過虛擬化的技術將資訊區隔開來；
3. 儲存地點不一定是貿易商的本國，貿易商與資訊可能分處在不同國家境內；
4. 同一個資訊的儲存地點可能不只一個，因雲端運算採分散式運算，資訊被散落在雲端各處，再透過強大的運算能力將其找出、提供給使用者，因此相同資訊很可能有多個儲存地點；
5. 雲端運算有許多分層，不同層次的系統多由不同服務提供者負責，是以在使用軟體或平台時，軟體或平台的服務提供者的工作有一部分可能被外包給第

[72] Jim Reavis et al., *Domain 9: Data Center Operations*, *in* SECURITY GUIDANCE FOR CRITICAL AREAS OF FOCUS IN CLOUD COMPUTING 59, 59 (Cloud Security Alliance ed., 2009).

三人，使用者無法掌握其資訊被受到如何之管理與處置[73]。這幾項特點，是傳統模式中較不常出現的狀況，在傳統模式中，資訊主要由企業自行持有，在整體網路環境中呈現分散的狀態。

貿易商透過 SaaS 模式與 PaaS 服務模式提供的資源為資訊之處理。SaaS 模式與 PaaS 模式的服務多存在於公用雲端上，雲端服務提供者通常為避免受到駭客侵入，對雲端的架構與資訊事項較為保密，使用者有時必須自行詢問，並且遵守保密合約，方才得以知道該雲端運算內與資訊來源、儲存相關的資料[74]。SaaS 模式與 PaaS 模式在提供服務時，可能涉及貿易商自有資訊之收集，譬如貿易商須提供其員工或客戶的個人資料，只是這些資訊被涵蓋在服務提供者隱藏的範圍內，呈現不透明的狀態[75]。貿易商須努力瞭解 SaaS 模式與 PaaS 模式中資訊被儲存的地點與情況，其原理與使用貿易雲端資料儲存服務時相同。

二、 貿易雲端的資訊安全威脅

貿易雲端的資訊安全問題大致上由幾種不同威脅造成。為求對雲端運算的資訊安全做有效管理，由 Google、Salesforce.com、Oracle、微軟公司等企業組成之 CSA，於 2010 年提出雲端運算安全的七大威脅，雖然這份研究並非特別針對貿易雲端提出，但對照貿易雲端與一般雲端運算的特性，CSA 提出的七大威脅，對貿易雲端服務之資訊安全造成影響，故仍有許多參考價值。

CSA 提出的雲端運算七大威脅包含：雲端運算遭人濫用或惡意使用；不安全的應用程式或開發介面；惡意的內部人員；共同基礎架構產生的問題；非蓄意之

[73] Jeff Spivey et al., *Domain 8: Traditional Security, Business Continuity and Disaster Recove*r, *in* SECURITY GUIDANCE FOR CRITICAL AREAS OF FOCUS IN CLOUD COMPUTING 55, 55-56 (Cloud Security Alliance ed., 2009).
[74] TIM MATHER et al., *supra* note 41, at 44-45.
[75] *Id*.; Jean Pawluk, *Domain 14: Storage*, *in* SECURITY GUIDANCE FOR CRITICAL AREAS OF FOCUS IN CLOUD COMPUTING 77, 77(Cloud Security Alliance ed., 2009).

資料外流；帳戶或服務被挾持；其他風險。以下分別敘述：

（一） 雲端運算遭人濫用或惡意使用

係指平台使用者或其他網路犯罪者利用雲端運算的基礎建設，從事不法行為，譬如製作並散布殭屍電腦網路、木馬病毒等，甚而透過殭屍網路控制整個 IaaS 伺服器，此舉可能引發其他電腦之防禦機制，導致雲端服務提供者成為被偵測、攻擊的目標，例如將該伺服器之資料當成垃圾資訊（spam）處理，使得該 IaaS 之網路位址（network address）被列入黑名單（blacklist）[76]。

（二） 不安全的應用程式或開發介面（API）

雲端服務提供者提供之 API 系統有漏洞，造成匿名者存取、重覆使用權利標識（token）或密碼、明文之內容傳輸（clear-text transmission of content），或資訊取得之控制系統僵化、不當授權、限制監管活動與登入權限等。此等現象將影響資訊之保密性、完整性與可用性[77]。

應用程式或開發介面與貿易商的 IT 系統不相容，亦可能產生資訊安全上的問題。若軟體及平台因此根本不合使用，貿易商無法從貿易雲端取得服務，若貿易商欲取得的服務是其獲得授權、可以取得與使用的資訊，則資訊的可用性為受到保障。

（三） 惡意的內部人員（Malicious insiders）

內部員工被授權服務與代管資訊系統，但雇用程序可能未被監督，導致有心

[76] *Top Threats to Cloud Computing V 1.0*, Cloud Security Alliance, Mar. 2010, at 8.
[77] *Id*., at 9.

人士得以滲透，員工蓄意竊取資料或資訊，以為個人目的、或售予他人。此將造成財務、生產力之損失，並且對品牌形象造成負面影響[78]。

（四） 共用基礎架構產生的問題

共用基礎架構對雲端服務使用者帶來的資訊安全疑慮，主要來自虛擬化技術。因虛擬化技術，一個硬體上可供不同資料共用，但系統若有弱點，可能導致不當存取客戶作業，或給與不當權限，影響資料之區隔，使沒有權限之人取得該等資訊[79]。申言之，不同資訊雖透過虛擬化技術為區隔，但當系統出現問題、譬如配置錯誤（misconfiguration）時，貿易商資訊仍可能被洩漏、或與其他資訊混淆[80]。

除來自服務提供者的錯誤、以及外部與內部的攻擊，貿易商亦可能面臨其他使用者造成的法律限制，間接導致其資訊安全受到侵害。這類情況包含依法得以監督、要求提供資訊，或法院的禁制令，譬如其他使用者因進入訴訟程序，法院對其相關設備為假扣押，導致該些硬體無法如常使用。此等情況可能損害資訊的保密性與可用性。

（五） 非蓄意之資料外流

因被網路釣魚侵入帳戶，或透過服務之弱點，控制該帳戶或服務。其將導致帳戶或服務被挾持，入侵者取得重要資、訊或得控制該服務，並損害資訊機密性、完整性，以及服務之可用性[81]。

---

[78] *Id*., at 10.
[79] *Id*., at 11.
[80] *Cloud Computing: Benefits, Risks and Recommendations for Information Security*, European Network and Information Security Agency, Nov. 2009, at 9.
[81] Cloud Security Alliance, *supra* note 76, at 12.

（六） 帳戶或服務被挾持

因被網路釣魚侵入帳戶、社交網站，或透過服務之弱點，控制該帳戶或服務。其將導致帳戶或服務被挾持，入侵者取得重要資、訊或得控制該服務，並損害資訊機密性、完整性，以及服務之可用性[82]。

（七） 其他風險

係不明的風險因素，可能是因與他人共用雲端資源、軟體相容性、軟體更新或資訊傳輸造成的損害。若網路服務提供者未遵守資訊安全相關守則或程序，定期查核並記錄，將使系統與資訊處在高風險狀態，即有可能造成損害[83]。

上述七點之外，雲端服務提供者之管理方式不當或無法及時，亦可能導致雲端運算之風險實現。在雲端運算模式下，服務提供者較能掌握資訊，若未妥善維護，或因維護導致資訊無法即時提供，或在處理資訊、升級或改版軟體與平台時造成資訊安全漏洞，皆可能提升雲端運算資訊風險[84]。

表 3　七大威脅影響之貿易雲端服務類型

	SaaS	PaaS	IaaS
雲端運算遭人濫用或惡意使用		O	O
不安全的應用程式或開發介面（API）	O	O	O
惡意的內部人員	O	O	O
共用基礎架構產生的問題	O		
非蓄意之資料外流	O	O	O

[82] *Id*., at 13.
[83] *Id*., at 14.
[84] Michael Armbrust et al, *supra* note 59, at 18; 高大宇等人，前揭註 54，頁 85-87。

帳戶或服務被挾持	O	O	O
其他風險	O	O	O

資料來源：*Top Threats to Cloud Computing V 1.0*, Cloud Security Alliance (2010).

當資訊安全風險實現時，將造成資訊之完整性、保密性與正確性受到破壞，導致貿易商資訊受到侵害。

第三節　貿易雲端與傳統模式下資訊安全問題之比較

傳統模式下，資訊安全亦為人們重視的一環。傳統電腦與網路以較為分散的方式處理資訊，通常由使用者自行維護主機與伺服器，購買軟體並安裝在個別主機上使用，使用者因此能自行掌握資訊。基於資訊呈現分散的狀態，企業雖然會遭逢電腦病毒、駭客入侵、系統故障等事件，但相較於雲端運算，傳統模式的資訊安全問題較為單純，也不容易擴散。

一、 傳統模式下之資訊安全問題

傳統模式下的資訊安全問題，其威脅可區分為來自內部或外部。資訊安全的內部風險包含人員、軟體、程式碼、風險管理上出現問題[85]，外部風險則來自網際網路中的侵犯，譬如網路病毒或駭客入侵[86]。對於導入電子商務的貿易商而言，其所使用之軟體、硬體及網際網路，皆可能受到這些威脅，導致資訊安全被破壞。有關傳統模式下資訊安全問題，說明如下：

[85] 高大宇等人，前揭註 54，頁 69-111。
[86] 同前註，頁 114-133，210-220。

（一） 網際網路資訊安全問題的內部威脅

1. 不良的內部人員

內部人員通常最瞭解系統，明白如何規避追查。在封閉性的網路中，仍不可避免不良內部人員帶來的資訊安全問題[87]。

2. 不良程式碼

不良程式碼之形成來自於設計者對系統的認知有限，導致程式碼設計無法達到良好的效果[88]。不良程式碼可能導致軟體功能不佳，或資訊安全有漏洞，在大型的應用軟體中，因程式碼較為複雜，軟體因此更可能存在大量安全缺陷[89]。

3. 不良的風險管理

不良的風險管理係指人員在開發或修改系統時，未完善地考量資訊安全風險，或者開發者或使用者有不良習慣，導致資訊安全問題發生，譬如公司內部資料流出[90]。

（二） 網際網路資訊安全問題的外部威脅

1. 電腦病毒

電腦病毒寄居在程式碼中，並且自我複製、繁殖與感染其他程式碼，其可破壞使用者的硬體與軟體設備。對電腦系統而言，電腦病毒會損害其安全性與完整性，並且占用硬碟空間；對資訊而言，電腦病毒可毀損、破壞（更

[87] 同前註，頁 87-88。
[88] 同前註，頁 88-94。
[89] 同前註。
[90] 同前註，頁 94-95。

改、加入不尋常錯誤）資訊，導致資訊無法被利用，且被破壞的資料無法被修復[91]。電腦病毒的種類包含檔案型病毒、開機型病毒、巨集型病毒、綜合型病毒等。這些病毒皆可透過網路方式流傳，且具備難以提防、未知、傳播速度快、型態多樣化、資訊損害大等特性[92]。

2. 網路駭客

網路駭客係指未經他人授權，侵入他人電腦系統竊取資訊、甚而破壞系統之人。駭客攻擊模式大致上可分為兩種，第一種為「被動式攻擊」，其目的在於取得資訊，因此會在避免資訊持有者得知的情況下偷聽或監看傳輸資訊[93]；第二種為「主動式攻擊」，除了竊取資訊，還涉及修改資料流的動作，使資訊之完整性受到損害[94]。

主動式網路駭客的攻擊手法包含冒充偽裝（masquerade）、重播（reply）、修改訊息與阻絕服務（denial of service, DOS）[95]。冒充偽裝係指冒充成另一個實體，並且配合其他攻擊模式採取行動，譬如攻擊者擷取有效認證程序，並且重播這個認證程序，以被攻擊者身分進入系統，進一步在系統中冒充更多身分。重播係指以被動式攻擊擷取資料後重新發送，使系統以為駭客是取得授權之人。修改訊息係指使正常情況下的訊息被做某些修改，例如修改機密資訊的讀取權限、修改網頁內容或介面。阻絕服務是駭客造成使用者無法正常使用或管理其設備，譬如封鎖前往某特定目的的交通，或者釋放大量訊息，增加系統負載量，導致網路或伺服器癱瘓。阻絕服務的攻擊通常具備特定攻擊目標[96]。

---

[91] 同前註，頁 118。
[92] 同前註，頁 119-122。
[93] WILLIAM STALLING 著，王金龍等譯，電腦網路　網際網路協定與技術，2006 年 1 月，頁 16-2 至 16-4。
[94] 同前註。
[95] 同前註。
[96] 同前註。

表 4 呈現出傳統模式資訊安全問題與威脅，指出大多數資訊安全風險實現，不外乎因軟體或系統出現設計上的漏洞，導致系統出錯，提升電腦病毒或駭客入侵的風險。又，若是在封閉的網路模式中，電腦病毒與駭客入侵風險應該較低，但無法避免惡意的內部人員竊取、竄改或破壞資訊。

表 4　傳統模式資訊安全問題與威脅

資訊安全問題	資訊安全問題的原因	可能減損的資訊安全功能與目的
資訊外洩	不良的內部人員、不良的風險管理、電腦病毒、駭客入侵	資訊保密性
資訊被竄改、破壞或毀損	不良的內部人員、不良程式碼、電腦病毒、駭客入侵	資訊保密性、完整性與可用性
因系統受干擾或入侵，導致資訊之處理與儲存產生安全疑慮	不良程式碼（例如緩衝區溢位，使安全性功能的記憶資料被其他資料覆寫，造成異常存取[97]）、不良的風險管理	資訊保密性、完整性與可用性
電腦系統受病毒破壞，造成電腦無法使用	電腦病毒、駭客入侵（放致病毒在電腦中）	資訊保密性、完整性與可用性

來源：本研究自製。

二、 貿易雲端與傳統模式之資訊安全問題比較

由貿易雲端與傳統模式資訊安全的原因中，可看出二者的資訊安全威脅大致

[97] 高大宇等人，前揭註 55，頁 90。

上相同（表 5），但因雲端運算模式、特性，在雲端運算模式下，有關服務提供者與服務使用者的行為，以及資訊儲存地點造成服務使用者面對自然環境或法規環境的風險，是採傳統模式較不被強調的部分。

表 5　貿易雲端與傳統模式資訊安全威脅之概念對照

貿易雲端資訊安全威脅	傳統模式資訊安全威脅
雲端運算遭人濫用或惡意使用	使用者或第三者之行為帶來的網路病毒；第三者若屬無權侵入，則該行為屬於駭客入侵。
不安全的應用程式或開發介面（API）	類似不良程式碼（兩者皆產生資訊安全漏洞）。
惡意的內部人員	不良的內部人員。
共用基礎架構產生的問題	類似不良程式碼、不良風險管理與網路病毒，前二者產生程式的資訊安全漏洞，病毒則可透過平台擴散。
非蓄意之資料外洩	不良程式碼、不良的風險管理造成資訊安全漏洞，而使網路病毒或駭客入侵。
帳戶或服務被挾持	網路病毒或駭客入侵。
其他風險	類似不良程式碼與不良風險管理，蓋這兩者產生的安全漏洞常是資訊人員預料之外的缺陷。

資料來源：本研究自製。

依貿易雲端與傳統模式架構、資訊儲存、分享的方式，可知貿易雲端與傳統模式資訊安全的不同之處，包含下列：

1. 貿易雲端資訊分布集中，儲存方式是透過虛擬化技術，將不同資訊在同一主

機上做區隔，是以遭受電腦病毒或駭客入侵時，其造成的損害程度可能大於傳統模式。

2. 貿易雲端使用的軟體與系統規模上大於傳統模式，其可能發生程式設計瑕疵及資訊安全漏洞，數量皆大於傳統模式[98]。
3. 貿易雲端的共用基礎架構，使得網路病毒入侵之機率、或其他資訊安全漏洞之數量增加，電腦病毒或其他資訊安全問題可能是由系統瑕疵或駭客入侵造成的，但也可能是內部其他使用者濫用或惡意使用所造成的。
4. 雲端運算的服務屬於長期性、連續性的服務，若服務業者退出市場，可能導致使用者資訊被刪除，或在移動資訊時產生額外風險與成本。
5. 使用者可能因濫用或其他過失行為，影響服務提供者與其他使用者之資訊安全。
6. 因資訊被儲存在眾多地點，且當中可能包含被儲存在國外，因此面臨更多環境風險、法律風險與政治風險。
7. 貿易雲端所存在的未知風險比傳統模式多。相較於傳統模式的資訊安全問題，貿易雲端無論就資訊安全的發生機率、發生後的損害，皆很可能大於傳統模式；在資訊安全管理事項上，導入貿易雲端的貿易商擁有較低的掌控能力，且處理的資訊安全問題比傳統模式複雜。

三、 降低或消除貿易雲端資訊安全風險的方法

資訊安全風險之控管，可透過技術、管理等方式，此外，政府若欲維護電腦與網路活動中的資訊安全，亦可透過制定法律或政策影響該環境。資訊安全之控管目的，主要基於「事前預防」之精神，希望藉此等活動降低或消除資訊安全風險（圖 10）。

[98] 同前註，頁 89。

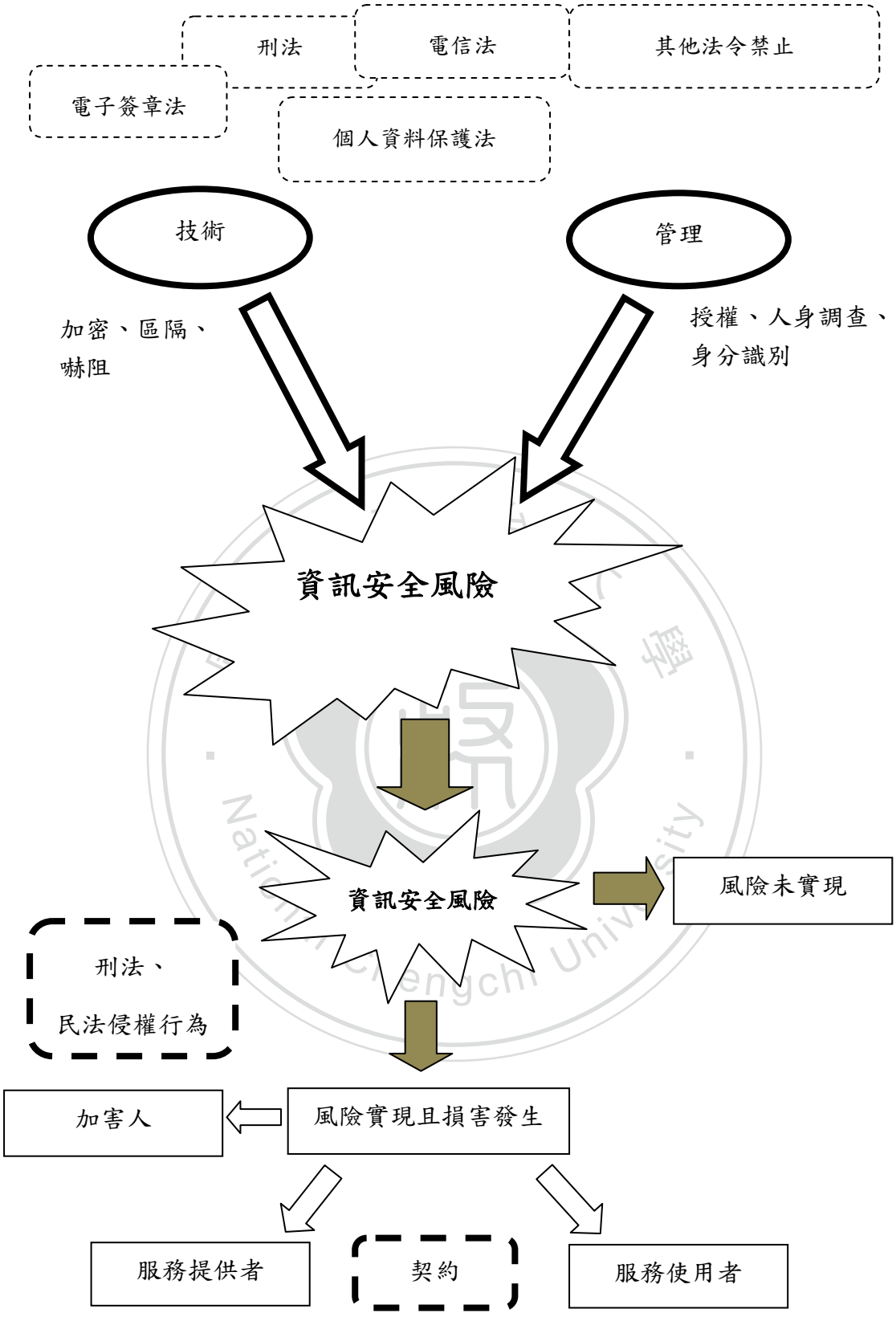

圖 10　雲端運算資訊安全風險之管理與分配

資料來源：本研究自製

本節就資訊安全威脅與風險之分類，歸納各種不同的控管方式。

（一） 傳統模式下既有之管理

在傳統模式下，人們可透過技術與管理方式控管資訊安全的威脅。有關內部人員存在的威脅，一般透過「人身調查」與「監督稽核」，分別針對處理敏感性資訊的員工與可疑的不當行為為觀察，以維護資訊之安全性[99]；有關程式碼的漏洞，以「檢查」、「稽核」與「分析」提升程式碼安全性，透過「檢查」避免遺漏程式中每個部份，透過「稽核」程式補強對入侵的防護，並且「分析」程式的缺失，以封鎖程式碼可能出現的安全漏洞[100]；有關不當的管理，管理者必須了解威脅存在於哪些事物上，並且對其資訊做隔離與備份，以在資訊安全風險實限時，可以將損害控制在最小範圍內[101]。

資訊安全的威脅有部分來自外界，常見者為駭客入侵與網路病毒。欲防止駭客入侵，系統可使用加密方式，確保資訊不被偷窺、竄改或公布等，確保資訊的保密性與完整性，具體的加密方式，包含授與金鑰、封裝安全承載等方式；對於主動式攻擊，在技術上可透過偵測，以及修復主動式攻擊造成的破壞，以對主動式攻擊造成嚇阻作用，進而確保其保密性、完整性與可用性之目的[102]。有關電腦病毒之防止，在技術層面上可透過病毒碼過濾法與加值總合法排除病毒，這兩種方式皆是以比對方式找出不尋常或有記錄的病毒程式碼[103]。此外，資訊業者與企業亦應指導其人員如何做好病毒防治，譬如建立正確使用習慣、定期備份與掃毒、拒絕開啟來路不明或可疑的檔案程式，以防止電腦病毒之感染或擴散[104]。

有關資訊安全相關管理方式，服務提供者可參考國際間對資訊安全管理做出

[99] 高大宇等人，前揭註 54，頁 96。
[100] 同前註，頁 100-101。
[101] 同前註，頁 109-110。
[102] WILLIAM STALLINGS，前揭註 93，頁 16-4。
[103] 高大宇等人，前揭註 54，頁 135-138。
[104] 同前註。

的建議與標準，例如技術基礎架構庫（IT Infrastructure Library, ITIL），用於規範 IT 服務管理架構，以提升 IT 服務水準，其中就資訊安全相關事項，有管理、控制取得授權、管理修補與配置等事項可供參考；ISO/IEC 27001/27002 則以 ITIL 為基礎，提供系統弱點管理、系統使用與取得之監管策略。透過 ITIL 與 ISO/IEC 27001/27002，使用者下之 IT 部門可在導入雲端運算時，確保現有之資訊安全程度與之符合，以及在導入後，應該以何種安全標準配合該些運作活動[105]。

（二） CSA 針對七大資訊安全威脅提出的解決方式

CSA 針對其所提出的七大資訊安全威脅的解決方式分別如下：

1. 雲端運算遭人濫用或惡意使用

有關雲端運算遭人濫用或惡意使用，主要透過管理方式解決，包含在初步審核與批准權限時採用較嚴格的標準；相關單位互相配合，提升對詐欺行為之監控；仔細檢視客戶網路通信狀況；監控公共的黑名單，並將之排除在自己的網路範圍之外[106]。

2. 不安全的應用程式或開發介面（API）

分析雲端服務提供者的介面及其所採用之安全模式；確保鑑定與取得資訊管道之強度，以及資訊傳輸時之加密；瞭解各個 API 之間的相關性[107]。

3. 惡意的內部人員

加強管理服務供應之每個環節，並且執行充分的評估；在契約或相關法律條款中納入人員選任之條件；要求服務提供者提升所有資訊安全與落實管

[105] TIM MATHER, *supra* note 41, at 112-113.
[106] Cloud Security Alliance, *supra* note 76.
[107] *Id*., at 9.

理之透明度，並且做相關報告；與服務提供者制定一通知程序，以供有破壞安全相關事項情事時為通知[108]。

4. 共用基礎架構產生的問題

採行對安全最有保障的存取與配置方式；監控環境中未經授權的改變與活動；在取得與處理服務的過程中推行強度的鑑定與控管；透過服務契約中之約定，要求修補與解決系統弱點；做弱點掃描與系統配置之審視[109]。

5. 非蓄意之資料外洩

對於 API 之取得採行較強之控管程度；在資訊傳輸時加密，以保障資訊之完整性；從設計面與運作過程中分析資訊之保護；採用較強度的金鑰、儲存與管理，並且就須銷毀的資料做徹底銷毀；透過契約要求服務提供者在將前人使用過的資訊系統或配件徹底清空後，方提供予其他人；透過契約要求服務提供者就備份與存取事項擬訂策略[110]。

6. 帳戶或服務被挾持

要求使用者與服務提供者相互提供證明文件；採用積極的監管系統，以偵測非經授權之活動；瞭解雲端服務安全相關政策與雲端服務契約內容[111]。

7. 其他風險

建議包含揭露可應用的記錄與資料；揭露可公布的基礎建設詳情；對必要資訊保持追蹤與警覺的態度[112]。

---

[108] *Id*., at 10.
[109] *Id*., at 11.
[110] *Id*., at 12.
[111] *Id*., at 13.
[112] *Id*., at 14.

（三） 透過法規影響

國際間對雲端運算或電子商務的法規尚未統一，各國之間就不同的電子商務或資訊安全問題立法。有關電子商務相關法規，目前各國大約採型三種立法模式，第一種為採用現行既有的法規，不就電子商務之交易特殊性為新立法必要；第二種為設立專法保護，此種法律將電子商務交易結合，制定單一法律，例如韓國的電子架構法（Framework Act on Electronic Commerce）、愛爾蘭電子商務法（Electronic Commerce Act of 2000）；第三種為折衷採行前兩種立法模式，僅在個別法律中修正與電子商務相關之條款，而未增訂新法[113]。

上述三種立法模式中，我國較常採第三種模式，因此與電子商務、乃至於電子相關資訊安全之處理，散見在個別法律中。我國與網際網路及雲端運算資訊安全問題相關之法律包含刑法、民法、電子簽章法、電信法等，分別對資訊各種基本目標與功能產生影響，如確保資訊不被盜用、個人資訊之蒐集與保護、電子文件完整性之確認等。其中，個人資訊之蒐集，與貿易活動較無相關，故以下分就刑法與民法、電子簽章法、電信法等為一概述。

1. 刑法、以及民法之侵權行為

刑法之作用包含保障人權、防衛社會、保護法益、矯治犯罪行為人等功能[114]。在保障資訊安全之情況中，因刑法明確規定犯了哪些事項構成罪、分別須受哪種程度的處罰，具有威嚇之作用，同時可成為該社會中人們的行為準則[115]。

資訊犯罪中與資訊安全相關者，包含竊取資訊、破壞或竄改資訊、毀損資訊，可能提升資訊風險者，則包含侵入電腦之行為、干擾電腦設備行為等。對此我國刑法於 2003 年修法時，增訂第 36 章「妨害電腦使用罪」及第 358

[113] 彭開英，日韓電子商務法制環境與發展之比較，科技法律透析，頁 41-42，2008 年 3 月。
[114] 黃仲夫，刑法精義，2006 年，頁 4-5。
[115] 同前註。

條至第 363 條。刑法第 358 條保護資訊不被無權之閱讀、存取、公布等，係保障資訊之保密性與完整性[116]；刑法第 359 條係保護資訊不被無權刪除、變更，係保障資訊之保密性、完整性與可用性[117]；刑法第 360 條保障資訊設備不受干擾，係保障資訊之保密性、完整性及可用性[118]。

若資訊安全犯罪導致損害發生，被害人依民法第 184 條規定請求損害賠償。就因資訊安全發生問題造成的財產方面損害，被害人得依民法第 184 條第 1 項前段規定,「因故意或過失,不法侵害他人之權利者,負損害賠償責任。」又，有關隱私權等其他權利被侵害時，依民法第 195 條第 1 項規定,「不法侵害他人之身體、健康、名譽、自由、信用、隱私、貞操，或不法侵害其他人格法益而情節重大者,被害人雖非財產上之損害,亦得請求賠償相當之金額。其名譽被侵害者，並得請求回覆名譽之適當處分。」民法上並未就隱私權設規定，惟依學者與實務之見解，公開揭露個人祕密係屬侵犯隱私權之一種態樣，因此在資訊安全受侵害時，若須以民法侵權行為為請求權基礎，應有適用之空間[119]。

2. 電子簽章法

電子簽章法之立法目的為確保電子交易之安全，促進電子化政府和電子商務的推展[120]。電子簽章法係透過電子簽章、數位簽章等不同方式，證明電子文件為真實且未經竄，進而確保資訊之保密性與完整性[121]。

依電子簽章法中對「電子簽章」和「數位簽章」的定義，前者係「依附於電子文件並與其相關連，用以辨識即確認電子文件簽署人身分、資格及電

[116] 我國刑法第 358 條:「無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或併科十萬元以下罰金。」
[117] 我國刑法第 359 條:「無故取得、刪除或變更他人電腦或其他相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。」
[118] 刑法第 360 條:「無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或併科十萬元以下罰金。」
[119] 王澤鑑，侵權行為法（1）－一般侵權行為，2006 年 8 月初版 11 刷，頁 151-153。
[120] 電子簽章法第 1 條。
[121] 電子簽章法第 2 條及第 9 條。

子文件真偽者[122]。」後者則為「將電子文件以數學演算法或其他方式運算為一定長度之數位資料，以簽署人之私密金鑰對其加密，形成電子簽章，並得以公開金鑰加以驗證者[123]。」以數位簽章簽署電子文件者，應由經許可之憑證機構依法簽發該憑證，憑證不得逾使用範圍為使用[124]；憑證機關就其相關作業導致當事人受有損害，或善意第三人因信賴該憑證而受有損害時，原則上推定其有過失[125]。此等規定係就電子文件之保密性有不同程度之保障。

3. 電信法

電信法立法目的之一為保障通信安全及維護使用者權益，其中並對電子商務之服務提供者設有規範[126]。電信法中與資訊安全相關之法條包含第 6 條及第 7 條，第 6 條規定電信事業應採適當且必要的措施，以保障其處理通信之祕密[127]；第 7 條規定電信事業及其服務人員應對電信之有無及其內容保守祕密，例外在法律規定時才得提供資訊[128]。此等規範皆為保障資訊安全。

我國之外，其他國家亦就資訊安全設有規範。美國除各州法律外，聯邦政府通過「醫療保險可攜與責任法（Health Insurance Portability and Accountability）」，針對個人醫療資訊之隱私權為立法保障[129]；歐盟之個人資料保護指令（Data Protection Directive, Directive 95/46/EC），則是規範企業使用者在收集個人資訊時，

[122] 電子簽章法第 2 條。
[123] 電子簽章法第 2 條。
[124] 電子簽章法第 10 條。
[125] 電子簽章法第 14 條第 1 項。
[126] 電信法第 1 條。
[127] 依電信法第 2 條之定義，「電信事業」係指經營電信服務供公眾使用之事業。依電信法第 11 條，電信事業包含第一類電信事業與第二類電信事業，第一類電信事業係指設置電信機線設備知事業，該電信機線設備指的是包含連接發信端與受信端之網路傳輸設備，與網路傳輸設備形成一體而設置的交換設備，以及二者間的附屬設備；第二類電信是非第一類電信之外其他事業，是以網路服務提供者，因其提供的內容為電信服務，但非電機線設備，屬於第二類電信事業。
[128] 電信法第 7 條。
[129] 宋佩珊，個人醫療資訊隱私權保護之立法趨勢探究－以美國、加拿大為例，科技法律透析，頁 46-47，2010 年 5 月。

其與資訊業者之間就該資訊之權利與責任劃分[130]。惟在貿易活動這類以 B2B 為主之活動中，此號指令之規範無法適用在貿易雲端之範圍。

第三節　小結

本章討論資訊安全風險與降低資訊安全風險之方式。資訊安全係指確保資訊之保密性、完整性、可用性、認證性與不可否認性，在貿易商活動中，因多數活動與資訊儲存或資訊處理相關，特別須重視期資訊之保密性、完整性與可用性。

本文在前半段部分檢視雲端運算之資訊安全風險，並且以其與傳統模式做比較，認為大部分造成風險的原因相同，相異並且引發疑慮者，為資訊儲存方式及資訊儲存地點。第二部分討論資訊安全之管理，主要探討如何透過管理、技術與法規等方式降低資訊安全風險，包含技術上加密、偵測等方式，以阻絕駭客攻擊，透過管理做監控、限制權限，並且要求服務提供者提供資訊安全相關通知，特別是在其安全發生問題時通知使用者。技術與管理之外，安全的電子商務環境亦可確保資訊安全，依我國規範，與資訊安全相關之法規散落在刑法、民法、電子簽章法與電信法等法律中。

資訊安全風險若不能透過管理、技術或法律影響等方式降低，則就其剩餘之風險應由何方承擔，應透過雙方契約之分配。此外，就有關資訊安全之管理部份，該等維護責任應由何方負責，亦須透過契約分配。此部分將於下一章闡述。

[130] 張乃文，雲端運算產業發展之策略規劃與法制因應，科技透析法律，頁 30，2010 年 12 月。

第四章　與貿易雲資訊安全相關之締約雙方責任分配暨現有雲端服務契約狀況

截至目前，各國針對雲端運算資訊安全所制定的法律有限。許多與資訊安全相關之法規，係針對傳統模式的網路犯罪、隱私權、電子文件傳輸所制定的規定，從法條上看起來，其功能似為嚇阻（例如刑法第 36 章），或幫助設立規範（例如電子簽章法中數位簽證須由憑證機構依法簽發），甚至做部分資訊安全維護責任分配（例如電信法第 6 條，電信業者有保障通信祕密的義務）。

當管理、技術與法規皆無法再降低或消除資訊安全的風險時，雲端運算使用者與服務提供者面臨資訊安全維護責任和損害分擔，包含平常時雙方各應盡哪些義務，當資訊安全風險實現時，其損失由誰承擔，此即為雲端運算契約必須處理的問題之一，是以貿易商在導入雲端運算時，就資訊安全管理的部分，須審慎檢視雲端服務契約內容。

本節舉出雲端運算契約訂定時，與資訊安全相關的注意事項，以及目前就雲端運算資訊安全提出的研究或建議中，其對責任分配模式之看法，另一方面，參考發展較完備之雲端運算服務提供者的服務契約、傳統模式下的產品與服務契約，最後參考我國業者就目前軟體、網路平台的實務運作上，就資訊安全是如何分配責任與損害，以觀察我國資訊業者對雲端運算資訊安全整體責任分擔的態度為何，並藉由這些事項，檢討與給與貿易商締約時的建議。

第一節　貿易雲資訊安全之責任分配與風險承擔

回顧第三章資訊安全的管理方法，CSA 在許多方法中強調使用者透過契約約定，以契約方式維護其資訊安全，例如要求服務提供者立即通知資訊安全發生

狀況。其他研究中，亦有強調雲端運算契約雙方應在契約中規範雙方責任，並認為詳盡的約定與遵守可提升使用者對服務提供者的信任程度[131]；ENISA 亦在其報告中建議，使用者應該妥適擬訂契約，透過契約管理其資訊安全風險[132]。

一、 貿易商在締結貿易雲端服務契約前之應有認知

貿易商在締結貿易雲端服務契約前，應認識雲端運算與傳統模式的差別，以及貿易商在不同雲端服務模式中所應負擔的責任，以免在導入貿易雲端後，承受太多不公平的對待。貿易商導入貿易雲端時，應意識到自己未來即將把重要的公司資訊、以及原本自由控制的電子商務事項交予貿易雲端，這種模式與傳統模式之間具極大差別。

有關資訊安全維護責任與損害承擔之分配，貿易商須自問，雲端服務提供者提供何種程度的資訊保護？資訊被儲存在哪些國家與機房?貿易雲端受到攻擊時，雲端服務提供者是否須通知貿易商？發生資訊安全問題、導致貿易商受有損害時，雲端服務提供者是否負擔完全的責任？若可歸責於雲端服務提供者，其是否能透過契約方式排除其責任？若雲端服務提供者須負損害賠償，雲端服務提供者對該賠償金額負擔無限責任還是有限責任？

二、 如何分配貿易雲端服務契約對資訊安全相關責任與損害

無論是何種服務模式，服務提供者與使用者皆無可避免地必須負擔一些責任，並風險實現時承受損害，是以雙方事前約定義務與責任範圍，對導入雲端運算而言非常重要。從雲端運算各種服務模式的技術層面觀察，SaaS 模式的服務提供

[131] TIM MATHER et al., supra note 41, at 109-110.
[132] ENISA, *Cloud Computing: Information Assurance Framework*, European Network and Information Security Agency 6 (2009).

者理所當然地須負擔大部分資訊安全的維護工作，原因在於服務提供者既把資訊全部集中在自己手上，對使用者的公開程度無法達到完全透明，且就算達到完全透明，能實質處裡資訊的仍是服務提供者[133]；PaaS 模式下，服務提供者與使用者應該分別就其平台與存放的應用程式負擔資訊安全責任，服務提供者主要負責其所提供之平台服務上的資訊安全，使用者則須對其放置應用程式的平台負擔與應用程式的資訊安全負責（圖 11）[134]；IaaS 模式下，服務提供者通常將使用者的資訊視為普通的物件，不清楚裡面的內容，導入這種服務模式的使用者多須自行維護所有資訊安全責任，就其下所提供給他人的應用程式與平台，其亦須負擔他們一部分的資訊安全維護責任[135]。

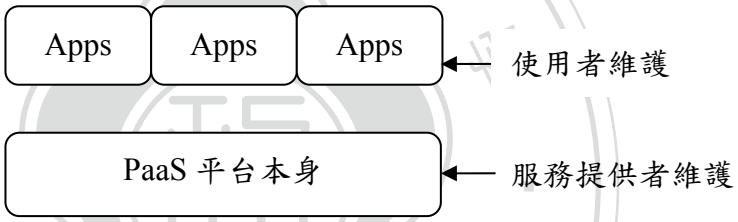

圖 11　PaaS 模式資訊安全責任之分擔
資料來源：本研究自製

歐洲網路和資訊安全機構（European Network and Information Security Agency, ENISA）就雲端服務契約中對責任分配的建議，主要依據雙方對資訊和設施的掌握程度，認為契約當事人應就其範圍內得控制的部分負責[136]。

貿易商導入不同雲端服務模式，將使其對貿易雲端資訊安全負擔不同程度的責任。論者普遍認為，資訊安全責任由掌控資訊與設施之人負責，在 SaaS 模式、PaaS 模式與 IaaS 模式中，貿易商有不同程度的控制權，尤其是前二者與 IaaS 模

[133] TIM MATHER et al., *supra* note 41, at 53-55.
[134] *Id*., at 56-57.
[135] *Id*., at 58-59.
[136] ENISA, *supra* note 132, at 8.

式之間有明顯之差異[137]。ENISA 在其報告中提出「對資訊或設施之掌控程度」為分配責任的判斷依據建議（表 6）。

表 6　雲端服務使用者與服務提供者對資訊安全相關事項的責任分配

	使用者	提供者
資訊內容的合法性	負全部責任	依既有法條之規定與其解釋，負中介商的責任
資訊安全發生問題（例如資訊外流、使用者帳戶被盜用等）	根據契約內容，就其所能控制的事項，為應盡之注意義務（due diligence）	就其所能控制的事項，為應盡之注意義務（due diligence）

資料來源：*Cloud Computing Information Assurance Framework*, ENISA, Nov. 2009.

表 7　SaaS 模式下雲端服務使用者與服務提供者之責任分配

使用者	提供者
1. 就蒐集客戶資訊乙節，遵行相關的資訊保護法律規範。 2. 維持身分認證管理系統。 3. 管理其身分認證管理系統。 4. 管理平台上的驗證機制（包含執行密碼驗證相關程序與規則）。	1. 維護支援平台的硬體設施（包含其設備、容量、電力、冷卻等事項）。 2. 維護硬體設施的安全與可用性（如伺服器、儲存功能、頻寬之狀況）。 3. 對作業系統的修復與補強（且考量使用者狀況使否與其相容，並提供適切的支援）。 4. 建構安全的平台，如制定與執行與防火牆相關的規範、調整 IDS／IPS[138]。

[137] *Id*.; TIM MATHER et al, *supra* note 41, at 53-59.

[138] IDS 係監測網路入侵檢測系統（intrusion detection system），主要功能為監測網路和／或系統活動中是否含有惡意活動、或違反規定的活動出現，並將偵測到的結果記錄、通報予技術人員；

	5. 監測系統。 6. 維持安全的平台，如維護防火牆、IDS／IPS、防止病毒入侵、採行封包過濾（packet filtering）等。 7. 記錄並監測安全相關事項。

資料來源：*Cloud Computing Information Assurance Framework*, ENISA, Nov. 2009.

表 8　PaaS 模式下雲端服務使用者與服務提供者之責任分配

服務使用者	服務提供者
1. 維持身分認證管理系統。 2. 管理其身分認證管理系統。 3. 管理平台上的驗證機制（包含執行密碼驗證相關程序與規則）。	1. 維護支援平台的硬體設施（包含其設備、容量、電力、冷卻等事項）。 2. 維護硬體設施的安全與可用性（如伺服器、儲存功能、頻寬之狀況）。 3. 對作業系統的修復與補強（且考量使用者狀況使否與其相容，並提供適切的支援）。 4. 建構安全的平台，如制定與執行與防火牆相關的規範、調整 IDS／IPS。 5. 監測系統。 6. 維持安全的平台，如維護防火牆、IDS／IPS、防止病毒入侵、採行封包過濾（packet filtering）等。

IPS 為入侵防禦系統（intrusion prevention system），其主要功能是檢測系統中的惡意活動，將此類活動區隔開來或停止下來，並且通報技術人員。參考資料：Wikipedia, *Intrusion detection system*, *at* http://en.wikipedia.org/wiki/Intrusion_detection_system (last visited Jul. 15, 2011); Wikipedia, *intrusion prevention system*, *at* http://en.wikipedia.org/wiki/Intrusion_prevention_system (last visited Jul. 15, 2011).

	7. 記錄並監測安全相關事項。

資料來源：*Cloud Computing Information Assurance Framework*, ENISA, Nov. 2009.

表 9　IaaS 模式下雲端服務使用者與服務提供者之責任分配

服務使用者	服務提供者
1. 維持身分認證管理系統。 2. 管理其身分認證管理系統。 3. 管理平台上的驗證機制（包含執行密碼驗證相關程序與規則）。 4. 對客戶作業系統的修復與補強（且考量客戶狀況使否與其相容，並提供適切的支援）。 5. 建構安全的平台供客戶使用，如制定與執行與防火牆相關的規範、調整 IDS／IPS。 6. 監測客戶的系統。 7. 對客戶維持安全的平台，如維護防火牆、IDS／IPS、防止病毒入侵、採行封包過濾（packet filtering）。 8. 記錄並監測安全相關事項。	1. 維護支援平台的硬體設施（包含其設備、容量、電力、冷卻等事項）。 2. 維護硬體設施的安全與可用性（如伺服器、儲存功能、頻寬之狀況）。 3. 負責主機系統（如管理系統、維持虛擬防火牆）。

資料來源：*Cloud Computing Information Assurance Framework*, ENISA, Nov. 2009.

由表 7、8、9 之比較，可觀察出導入 IaaS 模式的使用者，理論上幾乎對所有虛擬化部分的資訊安全負責，服務提供者所需負擔的，則只有硬體設備與主機系統狀態的維護與管理。

第二節　既有的雲端服務契約規範內容

與雲端運算資訊安全相關之法律問題，在法規之外，雲端運算服務之契約為雙方主要的主張依據，有參考之必要。有關雲端服務契約之訂定，實務上有雲端服務使用者挑選現成的契約，做其締約之主要架構與內容，再針對當中的某些條款與服務提供者協商，或甚至在無協商的情況下締結契約[139]。鑒於此一締約模式，加上許多雲端運算服務業者已發展出制式之契約內容，並且累積許多客戶，顯示出雙方就締約方式與契約本身之內容尚能接受，有關契約中之資訊安全責任分配，這些契約具有一定之參考價值。

本研究參考 Google、Salesforce.com（以下稱 Salesforce）、IBM、Windows Azure 與 Amazon AWS 之雲端服務契約，以觀察既有雲端服務契約規範架構、契約就維護資訊安全的責任分配、以及損害發生時損害賠償金額之決定等事項。選擇 Google、Salesforce.com、IBM、Microsoft 與 Amazon AWS 的原因有二，第一、這些公司已在國際間累積許多客戶；第二、這些公司皆提供 SaaS 與／或 PaaS 模式的服務，故具備參考價值，部分亦提供 IaaS 模式服務，可為與 SaaS 與／或 PaaS 模式比較之用。

一、　雲端服務提供者的服務暨相關資訊

本研究參考契約之雲端運算服務提供者，Google、Salesforce 與 Microsoft 的服務屬 SaaS 與／或 PaaS 模式，IBM 與 Amazon AWS 提供的服務包含 SaaS／PaaS 模式，亦包含 IaaS 模式的服務，服務涵蓋皆範圍包含商用雲端運算服務。

Google 的服務對象為一般大眾、企業與學校等不同機構，內容包含應用程式與平台。Google 提供給企業的雲端服務為 Google Apps for Business，企業可藉

[139] ENISA, *supra* note 132.

此取得電子信箱、文書編輯程式、資訊儲存空間、應用程式平台等服務。Google 的客戶對象涵蓋各種規模的公司，目前大約有 3 百萬家企業使用[140]。

Salesforce.com 主要提供 CRM 相關服務，其平台架構分為基礎環境、發展平台、社交平台與應用軟體。Salesforce.com 提供銷售管理應用程式、聯繫客戶的服務雲端、企業跨部門合作之雲端，以及建構商業應用程式的雲端平台，企業可使用該雲端服務的人次，規模可從 5 人擴充到 5,000 人，服務對象包含大型企業與中小企業[141]。

Windows Azure 是 Microsoft 公司的雲端運算產品，特色為幫助企業處理複雜的平台問題，讓企業專注於應用程式開發。Windows Azure 提供平台與 Windows Azure Tools for Microsoft Visual Studio，後者可幫助企業在 Windows Azure 上建立、設定、建置、偵錯、執行、封裝與部署可擴充的 Web 應用程式與服務[142]。

IBM 針對雲端運算提供的服務形式涵括雲端運算三種服務模式，並且包含私有雲端與公用雲端。IBM 認為雲端服務的導入程度，由淺到深分別為託管服務、私有雲服務、公用雲服務，企業可依其不同需求做不同搭配。為了滿足企業需求， IBM Smart Cloud 提供建置在企業防火牆，並由 IBM 代管的私有雲端，亦有將公用雲資源設置在私有雲端上的服務[143]。

Amazon 在 2006 年推出 Amazon Web Service（AWS），提供的服務涵括雲端運算三種服務模式。Amazon AWS 之 SaaS 模式提供電子商務流程所需之應用程式，包含 Fulfillment Web Service（FWS）、Flexible Payment Service（FPS）、Mechanical Turk 等；PaaS 模式之服務包含 Amazon Simple Queue Service（SQS）和 Amazon Simple Notification Service（SNS），可提供客戶資料暫存與使用，並

[140] 超過 3 百萬家公司選用 Google 應用服務，Google 網站，網址 http://www.google.com/apps/intl/zh-TW/business/index.html（最後瀏覽日期：2011 年 7 月 15 日）。
[141] Salesforce.com 官方網站，網址：http://www.salesforce.com/tw/ （最後瀏覽日期：2011 年 7 月 15 日）。
[142] Windows Azure Platform, *at* http://msdn.microsoft.com/zh-tw/windowsazure/ (last visited Jul. 15, 2011).
[143] 拓樸產業研究所，探索雲端運算市場新商機，2010 年，頁 34-36；IBM Smart Cloud, *at* http://www.ibm.com/cloud-computing/us/en/index.html (last visited Jul. 15, 2011).

且整合 Amazon 其他資源等用途；IaaS 模式之服務項目眾多，包含 Amazon Elastic Compute Cloud（Amazon EC2）、Simple Storage Service（Amazon S3）、Virtual Private Cloud（VPC）等，Amazon EC2 功能為雲端運算，Amazon S3 提供儲存服務，VPC 則提供私有雲端服務[144]。

二、 雲端運算服務契約之概要

雲端運算服務提供者在與服務使用者締約時，其契約常由不同契約與／或條款組成，並且以一個主要的服務契約（亦即雙方簽訂該條款或契約後，締結依雲端運算服務契約）將其他附屬條款包含進內容中，形成契約之全體，是以雙方所需遵守之義務與規範，不得僅參考契約之主要協議內容。常見的雲端運算契約包含主要的服務契約與服務層級契約（Service Level Agreement, SLA），締約雙方往往須一併遵守各國法律，以及該服務之網站使用規範、隱私權保護政策、智慧財產權保護政策等條款。

雲端運算服務的使用者，多半得依其需求使用雲端上的不同資源，因此在主要條款之外，契約可能包含其他 SLA。雲端運算服務提供者對不同使用者提供的服務類型與內容紛雜，且各項服務之範圍、程度、品質、期間等事項，亦有分別被明確化、具體化之必要，SLA 針對這些個別服務，規範雙方對該服務的合意細節，譬如服務應如何被執行、其品質應該到達何種程度等事項[145]。此外，因為服務提供者常與其它網路服務提供者合作，或使用其他服務提供者的服務，以執行 SLA 中的服務項目，是以締約雙方與第三方的關係，也間接影響該 SLA[146]。

本研究參考各個定型化契約之一般性規範，包含雙方在不同模式服務中的權利與義務、資訊安全責任分配及損害負擔程度等，故首要參考為主要的服務契約。

---

144 Amazon, Products & Services, *at* http://aws.amazon.com/products/ (last visited Oct. 1, 2011).
145 Li-jie Jin et al., *Analysis On Service Level Agreement Of Web Services*, Software Technology Laboratory of HP Laboratories Palo Alto (2002).
146 *Id*.

本研究所指之主要服務契約，其具體名稱並不相同，但皆關乎於締約雙方主要權利義務、責任分配與免除等事項。

本研究主要參考之雲端運算契約之一般性規定，包含下列：Google 之 Google Apps for Business 線上合約（Google Apps for Business Online），Salesforce 之 Salesforce 主要訂閱合約（Master Subscription Agreement）及 Salesforce 主要開發服務合約（Master Subscription Agreement Developer Services），Microsoft 之 Windows Azure Platform Consumption Online Subscription Agreement 及 Microsoft Online Services 使用權利，IBM 之 IBM Smart Business Cloud Agreement，以及 Amazon AWS 之 AWS Customer Agreement[147]。有關主要的服務協議與相關契約架構，如表 10 內容所載。

表 10　雲端服務提供模式與本研究探討之服務契約簡介

雲端運算服務提供者	服務提供模式	主要的服務契約條款（本研究主要探討內容）	主要服務契約條款外，契約其他部分、或締約雙方另應遵守者
Google	SaaS、PaaS	Google Apps for Business 線上合約（SaaS 和 PaaS 模式）	SLA、合理使用政策、網域服務使用條款等。
Salesforce	SaaS、PaaS	Salesforce 主要訂閱合約（SaaS 模式）；Salesforce 主要開發服務合約（PaaS 模式）	其他附件、主要服務契約條款之附約、訂購單等。

[147] 本研究中各項契約與條款名稱參考各雲端服務提供者之中譯名稱，若無中譯名稱，則從其原文。契約內容參考英文與中文版本，並以英文版本為主要參考依據。

Microsoft	PaaS	Windows Azure Platform Consumption Online Subscription Agreement、Microsoft Online Services 使用權利（PaaS 模式）	與主要服務契約條款相關之線上服務使用授權條款與相關產品授權使用條款、訂價單。
IBM	SaaS、PaaS、IaaS	IBM Smart Business Cloud Agreement	線上合理使用政策。
Amazon AWS	SaaS、PaaS、IaaS	AWS Customer Agreement	AWS Customer Agreement 外，契約意包含相關之 SLA。 契約之外，使用者須遵守服務條款、使用限制條款、隱私權政策等。

資料來源：本研究自行製作。

三、 雲端運算服務契約中之資訊安全維護義務分配

雲端運算之資訊安全維護義務之分配，多約定在主要服務協議，主要之服務協議中亦多規定雙方遵守隱私權保護政策、合理使用政策(Acceptable Use Policy)

等其他條款，以確保服務之安全性與品質。以下即以主要的服務協議為主要觀察對象，分別介紹 Google、Salesforce、Microsoft、IBM 及 Amazon 之定型化契約內容。

（一） Google Apps for Business 線上合約

Google Apps for Business 線上合約為 SaaS 模式與 PaaS 模式的服務，其服務主要依照 Google Apps for Business 合約及 Google 服務之各 SLA 的內容提供[148]。

依 Google Apps for Business 線上合約，Google 對「客戶（Customer）」除提供服務之外，就「客戶」資訊之處理、儲存、移動、修訂等事項，皆有相關約定[149]。有關「客戶」資訊的儲存與處理設施，Google 須以合理，並且不低於管理自有類似資訊儲存與處理設施的程度，以管理「客戶」資訊之設施。有關「客戶」資訊之安全性及完整性，Google 對其採行不低於業界標準的系統與程序，使該些資訊免於可預見的威脅、風險，並確保沒有未經授權之使用情況發生[150]。有關「客戶」之機密資訊，除有例外情況（例如不可歸責於接收者之公開、法規要求揭露等），原則上 Google 對於「客戶」之機密資訊負與管理自己事務相同程度的保護義務[151]。

「客戶」的義務包括相關條款之遵守、濫用情形之監控、相關管理權限之維護，以及對第三方之管理。「客戶」應遵守「合理使用政策（Acceptable Use Policy）」，在使用網域服務時，則應遵守「網域服務使用條款（Domain Service Terms）」[152]。「客戶」須監控、回應與處理傳送至濫用情形（abuse）與郵件管理員（postmaster）等客戶網域名稱別名（aliases for Customer Domain Names）的電子郵件[153]。「客

[148] Google Apps for Business Online Agreement, *at* http://www.google.com/apps/intl/en/terms/premier_terms.html (last visited Oct. 22, 2011).
[149] Google Apps for Business Online Agreement, art.1.1.
[150] Google Apps for Business Online Agreement, art.1.1.
[151] Google Apps for Business Online Agreement, art. 6.
[152] Google Apps for Business Online Agreement, art. 2.1.
[153] Google Apps for Business Online Agreement, art. 2.2.

戶」可指定具有管理帳戶（Admin Account）權限之人，負責內部管理工作[154]。「客戶」須以符合業界實務的方式，避免未被授權的使用，在發現有未授權使用之情事時，須終止之、並且通知 Google[155]。未經 Google 之書面同意，不得透過服務從事「高風險活動[156]」，亦不能透過服務儲存或傳輸法律規範下不得出口的「客戶」或「使用者（End User）[157]」資料[158]。就 Google 之機密資訊，「客戶」負擔與 Google 就「客戶」機密資訊相同之保護，原則上不得公開之[159]。

Google 若發現「使用者」有不當的使用，可要求「客戶」暫停「使用者」使用服務，若「客戶」未有效暫停該服務，Google 可以自行為之[160]。在緊急的安全情況發生時，Google 可先在最小範圍與最短時間內自動暫停與具攻擊性使用的服務，事後依「客戶」之要求為說明[161]。

契約終止時，有關資訊之處理易有規範。當契約終止，除服務之提供停止之外，Google 有返還「客戶」資料與「客戶」與刪除「客戶」資料之義務[162]。Google 與「客戶」皆負有以符合業界實務之方式歸還或銷毀對方機密資訊的義務[163]。

[154] Google Apps for Business Online Agreement, art. 2.3.
[155] Google Apps for Business Online Agreement, art. 2.5.
[156] 係指會造成人身傷亡或環境破壞的活動，譬如核子設施、空中交通系統、維生系統運作。Google Apps for Business Online Agreement, art.15.
[157] 係指「客戶」允許使用 Google Apps for Business 服務之人。Google Apps for Business Online Agreement, art.15.
[158] Google Apps for Business Online Agreement, art.2.6.
[159] Google Apps for Business Online Agreement, art. 6.
[160] Google Apps for Business Online Agreement, art. 5.1.
[161] Google Apps for Business Online Agreement, art. 5.2.
[162] Google Apps for Business Online Agreement, arts. 11.2(ii) (iii).
[163] Google Apps for Business Online Agreement, art. 11.2 (iv).

表 11　Google 契約雙方就資訊安全相關管理維護的責任

	Google	「客戶」
Google	1. 確保「客戶」資訊之保密性與完整性。 2. 返還並刪除「客戶」資料。 3. 對「客戶」之機密資訊為保護，並在契約終止後為歸還或銷毀。	1. 同意 Google 得處理資料。 2. 遵守相關條款。 3. 自行監控、回應與處理電子郵件之傳送。 4. 維護服務的管理功能。 5. 避免未授權使用之情形。 6. 不得使用服務從事高風險活動。 7. 不得在法規禁止時出口資料。 8. 對 Google 之機密資訊為保護，並在契約終止後為歸還或銷毀。。

資料來源：本研究自行製作

（二） Salesforce 主要訂閱合約與主要開發服務合約

Salesforce 主要有兩種服務契約，Salesforce 主要訂閱合約（Salesforce Master Subscription Agreement）為提供「客戶」取得與使用 Salesforec 網站上的服務，屬於 SaaS 模式；Salesforce 主要開發服務合約（Salesforce Master Subscription Agreement Developer Services）為提供「客戶」使用網站平台與應用程式開發、維持應用程式與服務，屬於 PaaS 模式。

1. Salesforce 主要訂閱合約

Salesforce 的義務包含隨時提供服務，以適當的方式保護「客戶」的資訊[164]。有關雲端運算服務內容，Salesforce 原則上隨時提供、更新改良[165]。有關「客戶」之資訊保護，Salesforce 以適當的管理、設備與技術防護措施保障其資訊安全[166]。契約終止後，Salesforce 負有返還資料與永久刪除資料之義務[167]。

「客戶」對資訊安全相關維護的義務，主要集中於管理自行之資料與其授權使用者之使用行為。「客戶」須確保其所授權之使用者遵行本服務合約內容；維持資料（Data）的正確性、合法性與品質；於合理商業範圍內防止未經授權的服務存取或服務使用，發現有未經授權之使用情事時，須通知 Salesforce；不得透過服務從事違法的行為（例如誹謗、侵犯隱私權等）；不得損害 Saleforce 服務或內含第三方資料之完整性或效能[168]。

前述義務之外，Salesforce 與「客戶」互負維護機密資訊、以及不得傳送惡意程式碼的義務。有關機密資訊之保護，一方保護對方之機密資訊，其保護程度必須與保護自有之同類機密資訊之程度相同，且不得低於一般人的合理注意義務（亦及善良管理人之注意程度）[169]。所謂「機密資訊」，包含服務、使用者的資料、合約條款、訂購單內容、雙方指明為機密資訊、以及就機密本質及公開情況，應合理地視為機密者[170]。有關惡意程式碼之禁止，雙方不得傳送惡意程式碼給對方，惡意程式碼包含病毒、蠕蟲、定時炸彈、特洛伊木馬程式及其他具傷害性或惡意之程式碼、檔案、指令碼、代理程式或程式[171]。

---

[164] Salesforce, Master Subscription Agreement, arts. 4.1 & 4.2, *available at* http://www.salesforce.com/company/legal/agreements.jsp (last visited Oct. 25, 2011).
[165] Salesforce, Master Subscription Agreement, art. 4.1.
[166] Salesforce, Master Subscription Agreement, art. 4.2.
[167] Salesforce, Master Subscription Agreement, arts. 12.4 &12.5.
[168] Salesforce, Master Subscription Agreement, art. 4.3.
[169] Salesforce, Master Subscription Agreement, art. 8.2.
[170] Salesforce, Master Subscription Agreement, art. 8.1.
[171] Salesforce, Master Subscription Agreement, arts. 4.3(d) & 9.1(iv).

2. Salesforce 主要開發服務合約

Salesforce 開發服務提供客戶自行開發程式與平台之服務，屬於 PaaS 模式之服務，有關其資訊安全相關規範，與 Salesforce 主要訂閱合約（SaaS 模式）之內容具有差別[172]。有關資訊保護之義務，Salesforce 主要開發服務合約中，並未就「客戶」資訊之保護與保護方式為明確之約定，相反的，在 Salesforce 主要訂閱合約（亦即 SaaS 模式）中，Salesforce 明確表示透過適當的管理、設施與技術，確保「客戶」資訊之安全[173]。有關雙方互負確保機密資訊安全之義務，其所謂之「機密資訊」，包含開發服務（the Developer Services），「客戶」的數據，「客戶」透過 Salesforce 服務所開發出之應用程式資料，或「客戶」存在於 Salesforce 平台的資料等，以及就個別服務內容所為之商業相關資訊，包含各條款、價金約定與訂購單內容等[174]。契約終止時，「客戶」可在 30 天內取回資料，且其使用 Salesforce 服務開發之應用程式或平台內容，將在契約終止後永久被刪除[175]。

Salesforce 就其 SaaS 模式與 PaaS 模式，分二個不同主要契約以為規範。比較兩分契約內容，可發現其大部分的資訊安全義務相同，包含 Salesforce 原則上應隨時提供服務，「客戶」應遵循相關條款，並且管理其下之使用者，以及雙方不得傳送惡意程式碼給對方，對「機密資訊」負保護之義務。除服務內容不同之外，SaaS 模式與 PaaS 模式之最大不同點，在於 PaaS 模式之契約中未就「客戶」資訊為明確之約定，故僅以 Salesforce 主要開發服務合約為判斷之依據，無法得知 Salesforce 是否對 PaaS 模式「客戶」的資訊負適當程度、或其它程度的注意義務。

---

[172] Salesforce, Master Subscription Agreement Developer Service, *available at* https://www.salesforce.com/company/legal/agreements.jsp (last visited Oct. 25, 2011).

[173] Salesforce, Master Subscription Agreement Developer Service, arts. 2&12.4; Salesforce, Master Subscription Agreement, art. 4.2.

[174] Salesforce, Master Subscription Agreement Developer Service, arts. 6.1 & 11.4.

[175] ; Salesforce, Master Subscription Agreement, arts.10.4&10.5.

表 12　Salesforce 契約雙方就資訊安全相關管理維護的責任

	Salesforce	「客戶」
Salesforce（SaaS）	1. 隨時提供服務。 2. 確保機密資訊之安全。 3. 對「客戶」資訊安全負適當的注意程度。 4. 不得傳送惡意程式碼。 5. 契約終止後，有依「客戶」在 30 日內提出的請求，透過令使用者下載方式返還其資料之義務。 6. 契約終止後永久刪除「客戶」資料。	1. 管理其內部人員遵行合約內容。 2. 管理使用權限。 3. 管理其所有內容之正確性、合法性與品質。 4. 不得使用服務從事違法行為。 5. 不得損害服務提供者或第三人服務之完整性與效能。 6. 確保機密資訊之安全。 7. 不得傳送惡意程式碼。
Salesforce（PaaS）	1. 隨時提供服務。 2. 確保機密資訊之安全。 3. 不得傳送惡意程式碼。 4. 契約終止後，有依「客戶」在 30 日內提出的請求，透過令使用者下載方式返還其資料之義務。 5. 契約終止後永久刪除「客戶」開發之應用程式及服務。	1. 管理其內部人員遵行合約內容。 2. 管理使用權限。 3. 管理其所有內容之正確性、合法性與品質。 4. 不得使用服務從事違法行為。 5. 不得損害服務提供者或第三人服務之完整性與效能。 6. 確保機密資訊之安全。 7. 不得傳送惡意程式碼。

資料來源：本研究自行製作。

（三） Microsoft 之 Windows Azure

Windows Azure 服務屬於 PaaS 模式服務，服務契約內容包括「Online Subscription Agreement」、「Microsoft Online Services 使用權利（Microsoft Online Services Use Rights）」，以及個別訂定的 SLA。Windows Azure 服務之資訊相關事項，多規範在 Microsoft 服務使用權利。

Online Subscription Agreement 中約定雙方義務。Window Azure 依照該條款與 Microsoft Online Services 使用權利提供服務[176]。雙方在履行契約義務時，基於合理範圍內無法控制之情事，譬如不可抗力、網際網路狀況、政府措施等事項所導致的履行不能，除客戶的付款義務之外，不用就其他債務不履行負其責任[177]。

Microsoft 與使用者間有關資訊之使用、管理與保存等事項，主要規範在 Microsoft Online Services 使用權利。依該條款，使用者一旦使用服務，即代表同意 Microsoft 收集、使用其相關資訊[178]。申言之，Microsoft 依「Microsoft 授權 資料傳輸通知（Microsoft Licensing Data Transfer Notices）」內容取得資料，其使用範圍包含基於改善產品服務，或幫助第三方改善其產品服務之目的，使用該等資料，但不得使用該等資料辨認或聯絡使用者[179]。提供與使用服務時，Microsoft 可能使用到使用者提供的客戶資訊（Customer Data），除非法律之要求，Microsoft 不會將該等客戶資訊揭露與第三人，並且救客戶資料之安全性實行合理及適當的措施，以協助保障這些資訊之安全性[180]。服務期限屆滿，使用者應通知 Microsoft 直接刪除或在保留期間內限制並保留其帳號，使用者表示刪除，或待保留期間期滿而使用者未為表示時，Microsoft 得在 30 日內刪除該使用者之資料，並且對該些資料不負保管、返還等責任[181]。

---

[176] Microsoft, Windows Azure Platform Consumption Online Subscription Agreement, art. 3, *available at* http://www.microsoft.com/online/mosa.aspx (last visited Oct. 25, 2011).
[177] Microsoft, Windows Azure Platform Consumption Online Subscription Agreement, art. 11(n).
[178] Microsoft, Microsoft Online Services Use Rights, Section A, art. I (h).
[179] Microsoft, Microsoft Online Services Use Rights, Section A, arts. I (h) (i) & (ii).
[180] Microsoft, Microsoft Online Services Use Rights, Section A, arts. III (p) & (q).
[181] Microsoft, Microsoft Online Services Use Rights, Section A, art. III (d).

使用者依 Microsoft Online Services 使用權利所負之義務，包含不濫用服務、維護帳號密碼之安全等事項。使用者不得濫用，或令他人未經授權之使用 Windows Azure 之服務[182]。使用者須維護其帳號密碼之機密性[183]。使用者不得透過服務為可能損害服務，或妨礙他人使用之行為，或者在未經授權之情況下，以任何方式試圖利用服務存取服務、資料、帳號等[184]。

表 13　Windows Azure 契約雙方就資訊安全相關管理維護的責任

	服務提供者	使用者
Windows Azure	1. 授權使用者使用。 2. 對客戶資訊安全之維護。	1. 取得授權後使用。 2. 不得濫用服務。 3. 維護帳號密碼。

資料來源：本研究自行製作

（四） IBM Smart Business Cloud Agreement

IBM 提供眾多類型的雲端服務，其中包含 IBM Smart Business Cloud，其所涉及之服務類型涵蓋所有雲端服務模式[185]。在 IBM Smart Business Cloud 下，IBM 提供平台給「客戶」經營，「客戶」可依該平台與 IBM 提供的服務，自行授權取得之人，其中包含可以「客戶」的帳號取得服務之「使用者（User）」，以及接收「客戶」提供之服務的「解決方案接收者（Solution Recipients）」。

IBM Smart Business Cloud 服務內容偏向 IaaS 模式，依其契約，IBM 提供「客戶」其所需的平台與支援服務，與「客戶」相關之資訊安全維護責任則多由「客

[182] Microsoft, Microsoft Online Services Use Rights, Section A, art. I (h) (iii).
[183] Microsoft, Microsoft Online Services Use Rights, Section A, art. III (f).
[184] Microsoft, Microsoft Online Services Use Rights, Section A, art. III (r).
[185] IBM Smart Cloud Overview, IBM, *at* http://www.ibm.com/cloud-computing/us/en/ (last visited Jul. 20, 2011).

戶」負擔[186]。「客戶」對於 IBM 服務與內容(Content)，除須遵守 IBM Smart Business Cloud Agreement 之外，同時須遵守各國法規、以及 IBM 合理使用政策(Acceptable Internet Use Policy for IBM Services）等條款規範[187]。「客戶」負責之資訊安全範圍，包含「客戶」或其相關人員（例如由「客戶」提供管道取得服務之「使用者（User)」及「解決方案接收者（Solution Recipients)」）所提供之數據、軟體、解決方案等事項。有關「內容」，「客戶」對其負全部責任，並且自行維護與備份等相關工作，倘若這些資訊中含有個人資料，其取得、處分與機密性維持等事項，亦為「客戶」之責任，IBM 不會將任何資料視為機密性資訊，並且以各種服務原有之安全性標準提供相關服務[188]。有關「客戶」授權「使用者」或「解決方案提供者」使用 IBM 服務或「內容」時，「客戶」須確保其締約與使用行為符合 IBM 條款之規範要求，換言之，「客戶」須確保其授權的使用活動遵行 IBM 相關條款，譬如 IBM 合理使用政策[189]。IBM 原則上不會取得或使用「內容」，例外在經「客戶」同意，或其目的係為提供服務，或法院要求提供時，方取得或使用之[190]。當有違反資訊安全規定等狀況發生時，若該狀況為緊急狀況，IBM 有權單方暫停服務之提供[191]。

表 14　IBM 契約雙方就資訊安全相關管理維護的責任

	服務提供者	「客戶」
IBM Smart Business Cloud	提供服務。	1. 遵守 IBM 條款、以及各國法律之規範。 2. 確保「使用者」與「解決

[186] IBM, IBM Smart Business Cloud Agreement, art 4. IBM 網路使用策略主要規範內容為禁止「客戶」透過網站或服務為某些行為，例如賭博，或公開或散布色情、暴力等題材之內容等事項。資料來源，IBM 網站，網址：http://www-935.ibm.com/services/us/imc/html/aup.html （最後瀏覽日：2011 年 11 月 15 日)。
[187] IBM, IBM Smart Business Cloud Agreement, art. 5.
[188] IBM, IBM Smart Business Cloud Agreement, art. 5.2.
[189] IBM, IBM Smart Business Cloud Agreement, art. 5.2.
[190] IBM, IBM Smart Business Cloud Agreement, art. 5.2.
[191] IBM, IBM Smart Business Cloud Agreement, art. 10.3.

		方案接收者」的行為都遵守其應遵守之條款或契約，且該條款或契約的保護程度不低於 IBM Smart Business Cloud Agreement。 3. 對其「內容」與相關個人資訊及其自身之機密資訊負責。 4. 明白 IBM 可因緊急狀況，單方暫停服務之提供。

資料來源：本研究自行製作

（五） Amazon AWS Customer Agreement

Amazon AWS 提供的服務包含 SaaS、PaaS 與 IaaS 模式，「客戶」基於 Amazon AWS Customer Agreement 以及實際使用到的 SLA，使用不同的服務模式。

依 AWS Customer Agreement，「內容（Content）」之所有權歸屬於「客戶」，而「客戶」對「內容」負相關之維護責任。「客戶」對其內容之責任包含維持技術相容，遵行法規與 AWS 和 Amazon 網站上的條款，處理第三人就「內容」所為之權利主張及相關訴訟[192]。有關「內容」的資訊安全，「客戶」應對其為妥善之安全性措施、保護、備份，包含對資訊加密，以防止未經授權之人取得[193]。「客

[192] Amazon, AWS Customer Agreement, arts. 8.1 & 4.1. 依該契約中第 14 條之定義，所謂「內容（Content）」，係指軟體、數據資料、文字、影音、圖像、或其他內容。
[193] Amazon, AWS Customer Agreement, art. 4.2.

戶」發現未經授權之人使用時，須將該情形通知 Amazon[194]。「客戶」須對最終使用者（End User）之使用行為負責[195]。

Amazon 負有提供服務，維護「客戶」「內容」之義務。Amazon 除提供服務外，須以合理適當之程度維護「客戶」「內容」，以避免發生意外的、或不合法的損失、取得與揭露。有關資訊之儲存，則應依照其隱私權保護政策規定，並由「客戶」決定「內容」之儲存地點與移動相關事項[196]。

有關 AWS 服務終止後之資訊處理，包含歸屬於「客戶」（即「內容」）或 Amazon（「AWS 內容」）兩種情況[197]。有關「內容」，Amazon 原則上不負返還義務，例外則由「客戶」與 Amazon 另達成合意、並在繳納價金與相關費用後，「客戶」方有權取回其在 AWS 服務下之「內容」[198]。有關「AWS 內容」，「客戶」負有返還，或依 Amazon 的指示為銷毀之義務。有關 Amazon 之機密資訊，「客戶」負有五年內不得揭露之義務[199]。

AWS Customer Agreement 之外，「客戶」須遵守 SLA、AWS Acceptable Use Policy、AWS Service Terms 等條款內容，這些條款中，亦就 Amazon 網站與其他 AWS 服務之資訊安全有相關規範，譬如 AWS Acceptable Use Policy 中，即規定 Amazon 網站之使用者不得未經授權取得或使用某些系統，以及 Amazon 就使用上之違規為監督與執行事項[200]。

表 15　Amazon AWS 之契約雙方就資訊安全相關管理維護的責任

	服務提供者	「客戶」
AWS Customer	1. 除條款第 10 條限制與客	1. 「客戶」發覺未經授權之

194 Amazon, AWS Customer Agreement, art. 1.2.
195 Amazon, AWS Customer Agreement, art. 4.3.
196 Amazon, AWS Customer Agreement, arts. 3.1 & 3.2.
197 依該契約中第 14 條之定義，所謂「AWS 內容（AWS Content）」，係就 AWS 服務或 Amazon 網站之取得與使用，Amazon 或其聯盟所提供的 WSDLs、文件、範例程式碼（sample code）、軟體集、命令列工具（command line tools）及其他相關技術。
198 Amazon, AWS Customer Agreement, art. 7.3 (b).
199 Amazon, AWS Customer Agreement, arts. 7.3 (a) (iii) & 13.1.
200 Amazon, AWS Acceptable Use Policy.

Agreement	戶在第 4.2 條的義務之外，對客戶的「內容（Content）」盡合理、適當的維護措施，以避免發生意外的、或不合法的損失、取得與揭露。 2. 客戶得選擇資訊之儲存地點與資訊移動之相關事項。 3. 原則上不負返還「內容」的義務，例外在與「客戶」另為合意、取得「客戶」支付服務終止後使用該服務之價金與相關費用後，提供其取回「內容」及相關協助。	人使用之情況時，通知 Amazon。 2. 負責「內容」之維護，包含技術上之相容性與法規條款等事項之遵循。 3. 對其「內容」為妥善之安全性措施、保護、備份，包含對資訊加密，以防止未經授權之人取得。 4. 管理最終使用者（End User）之使用。 5. 服務終止後，歸還，或依 Amazon 之指令銷毀所持有之「AWS 內容」。 6. 服務期間與服務終止後五年內，不得揭露 Amazon 機密資訊。 7. Amazon 在服務提供範圍內，依隱私權保護政策取得與處理客戶的資料與「內容」。

資料來源：本研究自行製作

由表 11 至表 15，可觀察出在 IaaS 模式之下，「客戶」需負擔較多資訊安全維護責任。在 SaaS 模式與 PaaS 模式，服務提供者須負擔確保機密之安全、資訊

環境之安全等事項，且多在契約終止後，提供一定時間內讓「客戶」要求歸還其資訊；反之，當所提供之服務偏向 IaaS 模式時，主要活動由「客戶」主導，因此其須對其內容、提供內容之對象的資訊與個人資料等事項負責。總結而言，不同服務模式下，服務提供者定型化契約就雙方對資訊安全責任分配之程度有明顯差異。

四、 雲端運算服務定型化契約之責任與免責相關條款

Google、Salesforce、Microsoft、IBM 及 Amazon 提供之定型化契約，除分配締約雙方的義務，也透過擔保條款、免責條款、有限責任條款、不可抗力因素條款，排除掉部分資訊安全責任或損害賠償負擔，是以使用者在締約前，亦須注意這些條款的內容與效力，檢視其是否將過度限制己方之求償權利。本節分別介紹、並比較五者之間對不同條款規範內容之異同。

（一） 擔保責任與免責聲明

有關雲端運算服務擔保責任與免責聲明，各雲端服務提供者之條款內容大致相同。雲端服務提供者多擔保依條款內容提供其服務，但除條款中明示的擔保之外，原則上不負擔任何明示、默示、法定或其他擔保責任，包含對適售性（merchantability）、適合特定用途（fitness for a particular purpose）擔保。擔保與免責條款之完整內容比較如表 16 所示。

由契約之擔保與免責條款，可知服務提供者依其在契約中之承諾提供服務，其服務內容以 SLA 或其他條款中之描述為準，不包含商業上適售性、供特定使用等特性。又，Google 與 Salesforce 對服務在停機時間時暫時提供乙節，已在其他條款中規定，而微軟公司的 Windows Azure 則是放在擔保內容中聲明。

表 16　各條款中的擔保及免責規範

	擔保內容	免責條款
Google	1. 雙方各自擁有完整的締約權力與權限[201]。 2. 雙方遵守所有適用於「服務」的法律與法規[202]。 3. Google根據相關之SLA內容提供服務[203]。	1. 除主要服務條款明示的事項，在適用法律允許範圍內，雙方不提出任何明示、暗示、法定或其他形式的擔保，包括（但不限於）就服務之商業適售性、特定目的適用性及未侵權的擔保[204]。 2. 就透過 Google「服務」提供或傳輸的內容或資訊，Google 本身不代表該些內容資訊之立場[205]。 3. 「客戶」了解「服務」並非以電話形式提供，且不可用於撥打或接聽電話，包含緊急服務電話和公開轉接的電話服務[206]。

[201] Google, Google Apps for Business Online Agreement, art. 9.1.
[202] Google, Google Apps for Business Online Agreement, art. 9.1.
[203] Google, Google Apps for Business Online Agreement, art. 9.1.
[204] Google, Google Apps for Business Online Agreement, art. 9.2.
[205] Google, Google Apps for Business Online Agreement, art. 9.2.
[206] Google, Google Apps for Business Online Agreement, art. 9.2.

Salesforce	SaaS	1. 合約雙方各自擁有完整的權力與權限簽署合約[207]。 2. Salesforce 依「使用者指南（the User Guide）」實質地執行服務提供；遵照第 5.3 節（Google 服務），在訂閱期間，「服務」在實質上不會有所減少[208]。 3. Salesforce 不傳送惡意程式碼給對方[209]。	除主要服務條款明示的事項，在適用法律允許的範圍內，雙方不提出任何明示、暗示、法定或其他形式之擔保，包括商業適售性、或特定目的之適用性的擔保[210]。
	PaaS	1. 合約雙方各自擁有完整的權力與權限簽署合約[211]。 2. Salesforce 依「使用者指南（the User Guide）」實質地執行服務提供；遵照第 3.3 節（與第三人提供之服務整合者），在訂閱期間，「服務」在實質上不會有所減少[212]。 3. Salesforce 不傳送惡意程式碼給對方[213]。	除主要服務條款明示的事項，在適用法律允許的範圍內，雙方不提出任何明示、暗示、法定或其他形式之擔保，包括商業適售性、或特定目的之適用性的擔保[214]。

[207] Salesforce, Master Subscription Agreement, art. 9.1& 9.2.
[208] Salesforce, Master Subscription Agreement, art.9.1.
[209] Salesforce, Master Subscription Agreement, art. 9.1.
[210] Salesforce, Master Subscription Agreement, art. 9.3.
[211] Salesforce, Master Subscription Agreement Developer Services, art. 7.
[212] Salesforce, Master Subscription Agreement Developer Services, art. 11.5.
[213] Salesforce, Master Subscription Agreement Developer Services, art. 11.5.
[214] Salesforce, Master Subscription Agreement Developer Services, art. 7.

Microsoft	1. 提供有限的擔保。擔保依契約描述內容，實質地提供服務給使用者，但該擔保受限於下列事項： i. 須在期限內； ii. 法律不容許排除的默示擔保、保證或條件，僅在擔保期限內提供； iii. 有限擔保範圍不包含使用者因意外、濫用或違反相關條款造成之問題； iv. 有限擔保範圍不包含使用者系統不支援的情況； v. 有限擔保範圍不包含因停機時間與其他中斷情況所造成的無法提供[215]。 2. 服務若未達到擔保範圍內之程度，Microsoft 退還一定期間內之繳款，或使服務升級至符合擔保範圍之程度。除非法律另有規定，否則 Microsoft 就擔保範圍事項不提供上述兩者以外之救濟[216]。	在適用法律容許範圍內，除條款中之有限擔保外，Microsoft 不做其他默示表述、擔保或條件，包含不針對適售性、就特定目的之適用性、滿意的品質等事項為擔保[217]。

[215] Microsoft, Windows Azure Platform Consumption Online Subscription Agreement, art.7 a.
[216] Microsoft, Windows Azure Platform Consumption Online Subscription Agreement, art.7 b.

IBM	無	無
Amazon AWS	Amazon 依照契約內容提供服務[218]。	1. Amazon、其聯盟夥伴及承包商不以任何形式，包含明示、暗示、法定或其他形式，而就服務提供或內容為擔保[219]。 2. Amazon 與其聯盟夥伴及承包商排除任何形式之擔保，包括服務之商業適售性、品質的滿意度、於特定目的之適用性、未侵權、享受、與交易之處理或效用相關之擔保[220]。

資料來源：本研究自製

（二） 不可抗力條款

雲端服務之定型化契約中，包含不可抗力條款（Force Majeure），以排除雙方或雲端服務提供者在某些情況下的契約義務或損害賠償責任。不可抗力條款中所約定之情況，指的是無法由契約當事人控制的情況，例如天災、戰亂、恐怖主義之行為等事項，在這些事項中，因契約當事人無法合理控制情勢，故不對債務不履行、或發生之損害負責。

本研究之研究對象中，僅 IBM 之定型化契約中無訂定不可抗力條款，而

[217] Microsoft, Windows Azure Platform Consumption Online Subscription Agreement, art.7 c.
[218] Amazon, AWS Customer Agreement, art. 10.
[219] Amazon, AWS Customer Agreement, art. 10.
[220] Amazon, AWS Customer Agreement, art. 10.

Google、Salesforce、Microsoft 與 Amazon 之不可抗力條款間，具有些微差異。依條文的體系架構，Google、Microsoft 和 Amazon 有單獨的不可抗力條款，Salesforce 則將該事項規範在 Salesforce 提供服務義務之例外情況，使用者並無適用不可抗力條款。依條文之適用對象，Google 與 Microsoft 之締約雙方皆適用不可抗力條款，而 Amazon 僅有服務提供者一方適用不可抗力條款。依條文排除的責任範圍，各個雲端服務提供者皆排除履行債務相關責任，惟 Microsoft 不排除使用者支付款責任，換言之，縱有不可抗力之情事，使用者仍須想辦法超越其合理控制範圍，以履行付款義務。

從資訊安全維護之角度觀察，雲端運算服務提供者之不可抗力條款，以 Google 與 Microsoft 不可抗力條款的適用範圍最大，對使用者最有利，相反地，Amazon 不可抗力條款的適用範圍最小，其僅排除服務提供者之責任，若服務使用者在合理控制範圍外有資訊安全受侵害之情事，造成 Amazon 之損害，服務使用者不得主張不可抗力條款。

表 17　雲端運算不可抗力條款

	不可抗力條款
Google	雙方就無法合理控制的任何因素（例如天災、戰爭、恐怖攻擊、暴動、勞資條件、政府行為與網路系統障礙）所造成之不當結果，無須承擔任何責任[221]。
Salesforce	原則上應隨時提供「購買之服務」的基本支援。例外時因情況超出 Salesforce 合理控制範圍所導致的無法使用狀態，包含但不限於天災、政府措施、洪水、火災、地震、動亂、恐怖攻擊、示威或其他勞工問題，或網際網路服務供應商故障或遲延時，排除 Salesforce 之隨時提供義務[222]。
Microsoft	雙方就無法合理控制的任何因素（例如火災、爆炸、停電、地震、洪水、暴風雨、罷工、禁運、勞工爭端、市民的或軍事機構的行動、戰爭、恐怖攻擊（包含網路恐怖攻擊）、不可抗力情形、網路流量廠商之作為或不作為、任何管理或政府機構之行為或不作為

[221] Google, Google Apps for Business Online Agreement, art. 14.4.
[222] Salesforce, Master Subscription Agreement, art. 4.1; Salesforce, Master Subscription Agreement Developer Services, art. 2.3.

	（包含通過法律、規則、或其他影響線上服務提供之政府行為)），導致該方當事人無法履行義務，任一方當事人無須對他方當事人負責。惟本規定內容不適用於客戶依本合約所負之付款義務[223]。
IBM	無
Amazon	Amazon 和其聯盟夥伴就無法合理控制之因素，不負延遲履行、或債務不履行的責任。「無法合理控制」之情形，包含了任何不可抗力情形、勞工爭端或產業中的動亂、電子系統，電信或其他設備損壞、地震、暴風雨、其他天災、阻塞、禁運、暴動、政府措施、恐怖攻擊或戰爭[224]。

資料來源：本研究自製。

（三） 雲端服務業者與使用者負擔之損害賠償責任

雲端服務服務提供者在其條款中約定其責任限制。服務提供者均約定其僅就因契約或與契約相關的直接損害負損害賠償責任，且對賠償金額設有上限。雲端服務提供者之定型化契約將損害賠償責任限制在直接責任，排除收益損失，或任何間接性、特殊性、隨附性（incidental）、衍生性、懲罰性或懲戒性（punitive），等間接性的責任。就賠償金額而言，該條款原則上有賠償金額上限，某些雲端服務業者在例外情況下不適用有限責任條款。有關各個定型化契約不同之處包含，第一、Google 和 Microsoft 之有限責任條款排除對保密義務、智慧財產權侵權之適用；第二、IBM 在其條款中強調不對客戶提供之資訊負擔毀損滅失責任，蓋在 IBM 與客戶間，有關客戶提供的資訊，係由客戶自行維護；第三、有限責任條款之適用主體不相同，Google、Salesforce 之 SaaS 模式服務、Microsoft 下，雙方皆得主張有限責任條款，然而在 Salesforce 之 PaaS 模式服務、IBM 與 Amazon，僅提供服務之一方得主張有限責任條款。

各契約有關損害之責任與賠償金額約定如表 18 與表 19 所示。

[223] Microsoft, Windows Azure Platform Consumption Online Subscription Agreement, art.11 n.
[224] Amazon, AWS Customer Agreement, art. 13.2.

表 18　雲端服務業者的責任限制

		責任限制範圍	責任限制條款適用範圍
Google		雙方不就收益損失，或任何間接性、特殊性、隨附性（incidental）、衍生性、懲罰性或懲戒性（punitive），承擔任何責任。即使對方已知悉或應當知悉該等損害的可能性，且該損害之直接損害賠償無法彌補損失，仍不需對其負責[225]。	1. 適用法律不容許時，不適用本條款[226]。 2. 本條款不適用於違反保密義務，或一方侵犯他方智慧財產權之行為[227]。
Salesforce	SaaS	雙方對於另一方之獲利或收益上之損失，或任何間接的、特殊的、附隨性、衍生性、涵蓋性或懲罰性損害，不論其是源於契約、侵權行為或其他責任理論，且不論對方是否被告知該損害的可能性，雙方均不負擔責任[228]。	在適用法律禁制範圍內，不適用本條款[229]。
	PaaS	Salesforce 對使用者獲利或收益上之損失，或任何間接的、特殊的、附隨性、衍生	在適用法律禁制範圍內，不適用本條款[231]。

[225] Google Apps for Business Online Agreement, art.13.1.
[226] Google Apps for Business Online Agreement, art. 13.3.
[227] Google Apps for Business Online Agreement, art. 13.3.
[228] Salesforce, Master Subscription Agreement, art. 11.2.
[229] Salesforce, Master Subscription Agreement, art. 11.2.
[231] Salesforce, Master Subscription Agreement Developer Services, art. 9.2.

		性、涵蓋性或懲罰性損害，不論其是源於契約、侵權行為或其他責任理論，且不論是否被告知該損害的可能性，皆不負擔責任[230]。	
Microsoft		1. 對客戶的賠償責任限縮在直接損害的責任[232]； 2. 雙方不負間接損害賠償負責，包含特殊的、或隨附性的損害，或獲利或利潤之損失，或商業資訊之損失。對方已被通知該可能性、或可預見該可能，亦同[233]。	1. 適用法律不容許時，不適用本條款[234]。 2. 此一有限責任條款不適用於違反保密義務，或一方侵犯他方智慧財產權之行為[235]。

[230] Salesforce, Master Subscription Agreement Developer Services, art. 9.2.
[232] Windows Azure Platform Consumption Online Subscription Agreement, art.9. a.
[233] Windows Azure Platform Consumption Online Subscription Agreement, art.9. b.
[234] Windows Azure Platform Consumption Online Subscription Agreement, art.9. b.
[235] Windows Azure Platform Consumption Online Subscription Agreement, art.9. b.

IBM	1. 就歸責於 IBM 之任何損害，不管其請求權為何，IBM 僅就其直接損害部分負擔賠償[236]。 2. IBM 不就客戶內容之毀損滅失負責[237]。 3. IBM 不就特殊的、隨附性、懲戒性的或間接的損害負經濟上責任[238]。 4. IBM 不就客戶獲利、商機、利潤、信譽與期待節省成本等之損失負責[239]。	1. 適用法律不容許時，不適用本條款[240]。 2. 人身損害（包含死亡）、或有形資產之損害不適用此條款[241]。
Amazon	1. Amazon 與其聯盟夥伴及承包商就直接的、間接的、附隨性、特別的、衍生性、懲罰性（包含獲利損失、信譽、用途、資訊所造成之損壞）之損害不負擔責任。縱一方被告知該損害可能性，亦同[242]。 2. Amazon 與其聯盟夥伴不	

[236] IBM, Smart Business Cloud Agreement, art. 12.1.
[237] IBM, Smart Business Cloud Agreement, art. 12.2.
[238] IBM, Smart Business Cloud Agreement, art. 12.2.
[239] IBM, Smart Business Cloud Agreement, art. 12.2.
[240] IBM, Smart Business Cloud Agreement, art. 12.
[241] IBM, Smart Business Cloud Agreement, art. 12.1.
[242] Amazon, AWS Customer Agreement, art. 11.

	就下列事項為賠償： （1） 因為服務被終止或暫停，或 Amazon 不再提供該服務，或在無預警或無計畫情況導致無法提供（如停電、系統故障等），而導致使用者無法使用服務； （2） 採購取代之產品或服務； （3） 使用者基於本契約、或為取得服務所為之任何投資、開支、承諾； （4） 使用者之內容或資料遭未經授權取得、變更、刪除、破壞、損害、喪失或儲存失敗[243]。	

資料來源：本研究自製。

表 19 雲端服務損害賠償上限金額

		責任限制金額
Google		雙方負擔的責任金額不超過客戶在事件前 12 個月內的支付金額[244]。
Salesforce	SaaS	因服務契約或與服務契約相關的雙方累計損害賠償責任，不管是依契約、侵

[243] Amazon, AWS Customer Agreement, art. 11.
[244] Google Apps for Business Online Agreement, art. 13.2.

		權行為或其他責任理論，均不超過使用者支付該服務的金額[245]；或 對單一事件，不得超過 50 萬美元、或事件前 12 個月內客戶依此支付的金額中之較低者[246]。
	PaaS	因服務契約或與服務契約相關的雙方累計損害賠償責任，不管是依契約、侵權行為或其他責任理論，均不超過 50 萬美元、或事件前 12 個月內客戶依此支付的金額中之較低者[247]。
Microsoft		1. 依何種責任理論構成的請求權，賠償金額共不超過使用者在「訂閱期間」或提出請求前 12 個月內客戶之支付金額中較低者[248]。 2. 有限賠償金額之約定不適用於： i. 雙方涉及「侵權及侵害索賠之辯護」乙節之 Microsoft 義務； ii. Microsoft、或其員工、或其代理人之重大過失或故意所致，並且得法院判定損害賠償責任； iii. 違反機密性條款下之義務； iv. 因 Microsoft、或其員工、或其代理人的過失造成人身傷亡情況，或因詐欺不實陳述引發之損害[249]。

[245] Salesforce, Master Subscription Agreement, art. 11.1.
[246] Salesforce, Master Subscription Agreement, art. 11.1.
[247] Salesforce, Master Subscription Agreement Developer Services, art. 9.1
[248] Windows Azure Platform Consumption Online Subscription Agreement, art.9. a.
[249] Windows Azure Platform Consumption Online Subscription Agreement, art.9. a.

IBM	IBM 就該直接損害之賠償金額不超過美金 25,000 元，或是客戶就該服務所支付的金額，若該支付為連續性，則以事件發生前 3 個月內客戶支付之金額為準[250]。
Amazon	Amazon 與其聯盟夥伴及承包商之總體損害賠償金額上限，為客戶就其所主張之服務、於事件發生後 12 個月內支付之金額[251]。

資料來源：本研究自製。

五、 雲端運算服務中就資訊安全責任之分配

觀察前述契約內容，有關資訊安全責任事項大致包含資訊之授權使用、資訊之保密性與完整性、資訊之儲存地點、契約終止時資訊之返還與銷毀等。在 SaaS 與 PaaS 模式下，雲端服務提供者負擔較多維護的責任，使用者多僅負維護身分資料、維護服務不被無授權之人使用，以及不使用服務為不當之運用，譬如違反法律、高風險行為、傳遞病毒等。由雙方負擔義務之形式，其與 ENISA 所建議之由「何人掌控、就由何人負責」模式類似。

有關擔保與免責條款，服務提供者多在契約中明示雙方的擔保事項，即依契約及契約相關條款提供服務，除此之外，多數服務提供者不就其它事項做任何形式的擔保，譬如服務的適售性、供特定用途的可用性等。代表服務提供者在維護之管理上，應依循條款或契約其他部分的規則進行，貿易商可藉此判斷該服務提供者對資訊安全的管理方式與保護程度。

[250] IBM, Smart Business Cloud Agreement, art. 12.1.
[251] Amazon, AWS Customer Agreement, art. 11.

有關不可抗力條款，服務提供者就履行契約、或者與契約相關之一切事項，排除單方或雙方在合理控制範圍外之責任。

有關責任限制條款，服務提供者多在契約中排除對衍生性與相關損害之責任，並且就其可歸責的部分約定限制金額。此外，在 IaaS 服務模式中，IBM 身為雲端服務提供者，不確保其客戶提出之資訊之毀損滅失，而在其他服務提供者、採 SaaS 模式與 PaaS 模式之情況，契約終止後服務提供者負返還義務。

雲端運算定型化契約之責任相關條款，其公平性與是否有效，皆值得懷疑，以下分別敘述。

1. 雲端運算定型化契約之責任相關條款是否公平

雲端運算服務提供者在其擔保事項中，多表示以 SLA 中之內容，確實提供服務，然而，各個 SLA 中對資訊安全之保障是否已足，使用者無法完全掌握，縱使雲端服務提供者違反其義務，依有限責任條款，使用者主張損害賠償的請求金額亦非採損失填補原則，因而僅能取得極為有限的金額，以 Salesforce 之 Sales Cloud 之價位為例，每月最高收費額為美金 250 元，以單一事件的損害賠償額計算方式，使用者主張損害賠償請求權，至多僅能獲得美金 3000 元，再考量資訊外洩之後果，包含使用者之商業機密、其下之個人資料等，皆可能被揭露、變更或為其他未經其授權之使用。基此，似難謂雲端運算服務提供者所設的賠償金額額度為合理或公平。

前述情況之外，雲端運算定型化契約條文中有關責任之條款，其共同產生之影響尚包含：第一、使用者之損害賠償請求權受到限制，蓋契約之責任條款排除掉許多責任事項，例如間接性的損害賠償責任、懲罰性賠償等；第二、某些服務提供者之定型化契約之主體為服務提供者，不包含使用者，故適用時僅排除服務提供者之責任，在可歸責於使用者之損害賠償情況，使用者不得主張免責條款或有限責任條款。

2. 雲端運算定型化契約之責任相關條款是否有效

雲端運算服務提供者透過定型化契約約定免責與有限責任條款，此等條款雖明文於契約中，卻不一定為有效，若法律禁止該等條款之適用，契約雙方即不得以該些條款為有效之主張或抗辯。雲端運算服務之擔保與免責條款，以及有限責任條款中，多半明文該條款在準據法容許時適用，又各國法律對有限責任條款效果之認定不同，是以在締結契約時，應注意契約約定的準據法與管轄法院為何，以求對己方最大的保障。以美國法為例，各州有明文禁止有限責任條款，亦有肯認有限責任條款者，前者如阿拉斯加州，後者如加州，依加州法院之 Markborough v. Superior Court 一案判決，當雙方議價能力相當或接近，並且適用範圍不涉及人身傷害，且限制責任的程度屬合理，加上雙方在締約時有談判交涉之機會，則認該有限責任條款為有效[252]。

假設雲端運算服務契約之準據法為我國法律，有關有限責任條款等約定，是否可構成民法第 247 條之 1？

依民法第 247 條之 1 規定，「依照當事人一方預定用於同類契約之條款而訂定之契約，為左列各款之約定，按其情形顯失公平者，該部分約定無效：一、免除或減輕預定契約條款之當事人之責任者。二、加重他方當事人之責任者。三、使他方當事人拋棄權利或限制其行使權利者。四、其他於他方當事人有重大不利益者。」

有關雲端服務契約中之有限責任，在雲端運算這種資訊集中在服務提供者一方、貿易商無法控制，且雙方公司規模懸殊之情況下，貿易商是否得主張此條款之內容？在第 247 條之 1 中，「按其情形顯失公平」係一不確定法律概念，應是個案而具體認定，並斟酌契約主要權利義務及法律規定而為判斷[253]。參考我國實務，最高法院 91 年度台再字第 45 號判決、以及 91 年度台上字第 2220 號判決內

[252] Howard W. Ashcraft et al., *Drafting Limitation of Liability Clauses: A Practical Guide for Design Professionals* (Feb., 2002), *available at* http://www.terrarrg.com/images/pdfs/DraftingLoL.pdf (last visited Nov. 20, 2011).

[253] 邱聰智，新訂民法債編通則（下），2003 年 3 月新訂一版，頁 139。

容，最高法院針對非消費性之活動的定型化契約是否顯失公平，表示「定型化契約之條款，因違反誠信原則，顯失公平而無效者，係以契約當事人之一方於訂約當時，處於無從選擇的對象或無拒絕締約餘地之情況，而簽訂顯然不利於己之約定為其要件。」然而依國際與國內之雲端運算市場發展，貿易商要達到「訂約當時，處於無從選擇的對象或無拒絕締約餘地之情況」似乎仍不太可能，不一定構成「按其情形顯失公平」，加上資訊安全風險不一定會發生，有關對資訊安全風險實現之損害負有限責任，是否屬於「顯然不利於己之約定為其要件」，也屬於尚未確定、必須進一步討論的範圍。

第三節　我國與貿易相關的傳統電腦與網路服務契約

我國目前尚未有如 Google、Salesforce、Windows Azure 或 IBM 一類之雲端服務提供者，較與雲端運算相關的產業，多為發展雲端運算之基礎設施，或對一般消費大眾[254]。就貿易雲端而言，與貿易雲端服務具替代關係的電腦與網路服務包含軟體開發、軟體產品、硬體設施、應用服務提供（Application Service Provider, ASP）網際網路平台等項目。以下參考行政院主計處提供之電腦軟體與硬體相關參考合約，一般網路平台規範條款，以及關貿網路使用規範，並透過訪談，以對我國資訊業與貿易商締約過程與責任分被有更多瞭解。

一、　傳統模式之契約架構與責任分配

我國目前的貿易電子商務環境，相關的資訊業者就軟體、網路平台為分工，其中有業者締結契約時，係參考行政院主計處提供之契約範本，以其為締約時參

[254] 作者訪談內容。

考的依據[255]。此外，關貿網路設有關貿網路使用規範，當中規定服務提供者與服務使用者之權利義務與責任歸屬，亦據參考價值。

（一） 行政院主計處就電腦硬體與軟體設備提供之參考合約範本

行政院主計處提供之參考合約範本包含：電腦硬體設備採購、電腦硬體設備租賃、電腦硬體設備維護、電腦軟體授權使用、電腦軟體委託開發之業務，提供參考合約範本[256]。

依行政院主計處之參考合約範本，有關雙方義務，在電腦硬體設備採購、電腦硬體設備租賃、電腦軟體授權使用之情況，其所交易之標的皆為「產品」。在電腦硬體設備採購之情況，買方負有採購前準備空間、點收、測試、驗收之義務，賣方在保固期限內負有保固服務義務[257]；在電腦硬體租賃之情況，租方負場地準備、點收、測試、驗收、契約終止時返還設備等義務，賃方須負維護設備之義務[258]；在電腦軟體授權使用情況中，軟體授權方提供授權予對方，但未就其故障時之修復為約定條款。有關電腦硬體維護與電腦軟體開發，則係企業委由資訊業者負責維修或開發軟體程式之勞務。

有關損害賠償，參考合約範本中的約定皆為資訊業者就其實質損害負擔有限責任，損害賠償金額可能是產品價格、勞務價格，或產品使用期間支付之金額等，譬如電腦軟體委託開發參考合約第 13 條規定，「雙方所得請求之損害賠償以實際損害為限，且以造成損害之個別專案開發費用百分之　為限。」其他參考合約就其損害賠償部分，亦以類似之架構限縮資訊業者損害賠償責任[259]。

---

[255] 例如介宏資訊有限公司。資料來源：電話詢問。

[256] 行政院主計處，參考合約，網址：http://www.dgbas.gov.tw/lp.asp?ctNode=2289&CtUnit=1075&BaseDSD=7&mp=1（最後瀏覽日期：2011 年 7 月 20 日）。

[257] 行政院主計處電腦硬體設備採購參考合約，第 4 條，第 6 條，第 8 條，第 9 條，第 14 條。

[258] 行政院主計處電腦硬體設備租賃參考合約，第 6 條，第 8 條，第 10 條，第 14 條，第 17 條。

[259] 行政院主計處電腦硬體設備採購參考合約第 17 條;行政院主計處電腦硬體設備租賃參考合約第 18 條：行政院主計處電腦硬體設備維護參考合約第 6 條：行政院主計處電腦軟體授權使用參

（二） 關貿網路使用規範

關貿網路提供企業各類型加值服務，申言之，其透過系統幫助企業處理資料，再回覆給企業保存使用。關貿網路一開始係從貿易便捷化相關服務起家，進而發展出對不同物流業者、零售與批發業者、乃至於一般企業，提供各類型加值服務系統[260]。

關貿網路的服務契約包含「關貿網路使用規範」條款[261]。關貿網路使用規範條款中有關資訊與資訊安全之規定，包含使用者以電子簽章法規定製作與傳輸資料，遵守系統使用規則，對關貿網路負有保密義務，處理資訊時不得牴觸法令與國令政策，為使用其電腦網路之第三人行為以及其所外伸之第三人網路業者之行為負責[262]。關貿網路提供使用者服務內容，維持系統運作於良好狀態[263]。

關貿網路就其系統故障負修復之責任，其僅就關貿網路有故意或重大過失、並可歸責於關貿網路的系統故障，其所導致的直接損害，方由關貿網站負擔損害賠償責任。關貿網路就其賠償負擔有限責任，賠償金額一次不超過新台幣 30 萬元，或十二個月內連續發生損害賠償事故，賠償累積數額不超過 60 萬元[264]。

關貿網路對非其所造成之損害，或因使用者未遵守其所指示之規定，或非由其提供或維修之產品瑕疵，或因天災或不可抗力造成之無法履行或不完全履行，亦不負責[265]。

（三） 其他網路平台規範條款

貿易商可能使用之電子商務尚包含其他軟體與網站，就網站之使用，許多網

考合約第 9 條；行政院主計處電腦軟體委託開發參考合約第 13 條。

[260] 關貿網路網站，網址：http://www.tradevan.com.tw/web/guest/home（2011 年 7 月 20 日）。

[261] 關貿網路使用規範第 28 條第 1 項。

[262] 關貿網路使用規範第 5 條，第 6 條，第 15 條，第 17 條，第 26 條，第 27 條。

[263] 關貿網路使用條款第 9 條第 1 項。

[264] 關貿網路使用規範第 9 條第 2 項與第 7 項。

[265] 關貿網路使用規範第 9 條第 8 項。

站幫助貿易商收集商情，亦或提供其電子交易之平台。就現有之電子商務交易平台，無論是 B2B 或 B2C 模式，網站服務提供者通常強調其本身之中立性，不介入使用者之間的買賣關係，亦不就張貼訊息的正確性負責[266]。此外，此等網站亦有免責聲明與有限責任條款[267]。

二、 對資訊業者就資訊安全事項之訪談內容

基於取得之契約文件有限，本研究進行二次訪談，對象皆為資訊業者。以下就訪談內容提出對企業締約、責任分配及資訊安全相關事項之訪談結果。

（一） 關貿網路

關貿網路締約模式，雙方主要遵循關貿網路使用規範。有關雙方對資訊之處置，關貿網路負有在一定期間內保管客戶資訊之義務。資訊之所有者為客戶，客戶若要使用服務，須授權關貿網路為其處理。其他與資訊安全損害發生與損害賠償等情事，皆依照關貿網路使用規範第 9 條關貿網站責任之規範處理。有關第 9 條第 2 項，「乙方（關貿網站）對於甲方（使用者）因本系統故障所至直接損害，除系統故障原因之發生，依其情形，顯然可歸責於乙方者外，免負賠償責任。」關貿網路就其可歸責之系統故障，所指之直接損害，係指因系統故障導致某些活動無法進行而造成之損失，譬如通關時具急迫性，若此時關貿網路系統故障，導致損害發生，則關貿網路在其可歸責情況下就該損失負擔賠償責任。

有關貿易業者是否對資訊安全產生疑慮，受訪者表示業者對資訊安全疑慮是必然情形，然而依其服務性質，貿易業者須將資訊交由關貿網路處理。關貿網路為消除客戶疑慮，主要是透過完善的管理與技術防範資訊安全問題，並且提供客

[266] 例如台灣經貿網供應商會員合約第 7 條；露天會員拍賣合約第 3 條，第 5 條。
[267] 例如台灣經貿網供應商會員合約第 10 條；露天會員拍賣合約第 9 條。

戶其資訊備份。截至目前，關貿網路尚未因資訊安全問題引起訴訟。

（二） 介宏資訊有限公司

介宏資訊為提供企業軟體之公司，在貿易活動中，多提供物流業者系統與服務。介宏資訊締約模式為分別跟不同客戶締約，而非使用定型化契約規定彼此權利義務，是以每份契約異質性相對較高，並且具保密性，無法提供研究參考。

介宏資訊將其系統以產品方式賣給客戶，並約定產品使用期間、產品保固期間，在保固期間之內，介宏資訊提供免費維修服務，保固期過了之後，若客戶欲繼續使用維修服務，則需另行與介宏資訊訂定維護契約。

介宏資訊之軟體買賣契約範本僅規定雙方權利義務、產品使用期間、準據法與管轄法院等事項，並未另約定免責條款或有限責任條款。然而實務上，介宏與客戶就其有限責任有約定，通常參考維護契約之支付金額，以為賠償金額之上限，若客戶不接受有限責任條款，介宏資訊可能寧願選擇不要締約。會有此一現象，一方面因介宏資訊的締約對象較少，共約 200 多個廠商，產品類型單純，再加上書面契約在此僅提供參考依據之功能，是以書面記載的可能僅為契約一部分內容，其形式簡單。

介宏資訊對資訊與資訊安全之維護，就資訊本身，介宏資訊僅幫忙處理資訊，而不存取該些資訊，因此若是資訊在處理過程中遭受毀損，歸責於介宏資訊，但若資訊之毀損滅失發生在存取的時間中，因非介宏資訊與客戶契約範圍內，自然與介宏資訊無關。有關資訊安全之維護，除落實資訊安全管理之外，當系統故障時，介宏資訊會及時在短時間內將系統修復。介宏資訊目前亦無發生重大資訊安全問題，且與客戶之間亦未就資訊與資訊安全相關問題發生訴訟。

三、　雲端服務契約與傳統模式責任分配之不同

雲端服務契約與傳統模式之責任分配，就免責條款與有限責任等概念基本上相同，不同之處似在於提供標的為「產品」或「服務」；雙方就資訊、授權、維護身分辨識等事項上，以雲端服務契約及關貿網站使用規範相比，前者的權利義務劃分約定事項較多，包含其客戶以下所有相關使用人需經授權而使用、必須遵守相同條款內容等。會有此等差別，並非關貿網站使用規範不夠詳細，而係因雲端服務契約可能包含不同模式與不同種類之服務，且其允許客戶就其服務或平台發展成新的應用程式或其他服務，並提供給第三方，這部分為關貿網路與傳統模式下多半沒有的。在傳統模式下，資訊之硬體與軟體多以產品形式出售，在物理上僅能供該客戶使用，若是在網路上取得並使用的系統，資訊業者多也限制客戶使用之權限，或者因第三方使用與其客戶完全相同之服務，可直接約定客戶對從其延伸出去之事項對資訊業者負責。

就免責條款與有限責任，由行政院之參考合約，可推知我國政府並未就雙方責任分配做限制或建議，須由契約雙方自行協商訂定，此外，我國並無反對有限責任條款之有效性。

第四節　小結

本章探討雲端運算資訊安全風險之責任分配。為瞭解並檢討一問題，本章先參考學者與 ENISA 對資訊安全責任分配之建議與模式，並得出 SaaS 模式與 PaaS 模式因技術上服務提供者較能控制，服務提供者就維護資訊安全而言負較多責任。本章參考 Google、Salesforce、Windows Azure、IBM 與 Amazon 提供之不同形式雲端服務契約，發現此等契約的責任分配大致上與理論所建議的相同，且就風險實現後之損害，雲端服務業者透過免責條款與有限責任條款，將其責任做出限縮。

有關此等免責條款與有限責任條款，貿易商在締約時應注意該契約準據法之適用，以及該準據法下對此等條款之效力認定。假設準據法為我國，此等條款是否具有效性，有關免責條款，一方面條文未明文禁止，二來參考合約範本中亦無建議，似可判斷出對雙方當事人責任分配問題採尊重契約自由之立場，由契約雙方自行分配責任。有關有限責任條款，我國行政院提供之參考合約範本就有限責任條款有類似規定，故可推測其具有效性。

依我國實務界之經驗，其與客戶訂定契約時，不一定會明文免責條款或有限責任條款，但就有限責任條款，資訊業者與其客戶可能在協商過程中約定，若資訊業者須對該契約負擔無限責任，可能造成進入契約之阻力，使資訊業者寧可選擇放棄締約。

就目前雲端服務條款與傳統模式條款內容，其不同之處主要為交易標的不同，以及就雙方責任分配事項上，雲端服務條款花費較多篇幅約定資訊安全管理義務之分配。然而契約主要架構仍差不多，且服務提供者與資訊業者皆在條款中做出限縮己方損害賠償責任之約定。

第五章　結論暨評論與建議

本章就先前之討論與比較，得出以下結論與建議。

第一節　結論

一、　我國應針對貿易商特性建制適合之貿易雲端

對我國貿易商而言，導入雲端運算，應為一邁入電子商務、進而提升競爭力之理想模式。近年來，我國貿易商面臨自由貿易蓬勃、廠商垂直整合、去中間化等趨勢，必須想辦法提升其國際競爭力，而導入電子商務，被認為是可提升商業效率、降低運籌成本之方式。電子商務可透過不同技術與模式呈現，在各種方式之中，雲端運算具有低投入成本、高效率、無須費太多心力維護系統等優點，考量我國貿易商多為中小型企業，其規模與研發能力有限，雲端運算為貿易商可採用的理想電子商務模式。

截至目前，我國雲端運算相關計畫仍在發展階段，且貿易雲端計畫停擺，其概念與架構尚不清楚。參考我國經濟部與國際貿易局先前之提案，同時考量貿易雲端欲達成之目的、吸引廠商之誘因、我國貿易商之特性，本研究認為貿易雲端須納入貿易流程中所有參與者與活動，並且與國際接軌，以達到貿易雲端之綜效，並吸引更多貿易商加入。此外，就貿易雲端之開放性，基於貿易商有部分資訊不適合公開，故應採混合雲端模式導入。

二、 貿易雲端資訊安全相關事項

貿易商不願導入雲端運算之原因，有一大部分係基於資訊安全考量。依雲端運算模式，雲端服務提供者透過多租戶架構方式，集中保管所有貿易商的資訊，申言之，不同貿易商的資訊被以虛擬化方式儲存在同一硬體上。此一特性足以使貿易商對雲端運算的資訊安全存疑。

比較貿易雲端與傳統模式之資訊安全事項，無論是其所受到的威脅，亦或確保資訊安全的方式，二者大致上相同。有關資訊安全受到的威脅，包含來自於惡意內部人員、不良的程式產生的漏洞，對外的威脅則包含電腦病毒與駭客入侵等，惟貿易雲端因其存取資訊方式，加上資訊必須常常被傳遞，這種遠距、集中、共享之模式，使其受到其他使用者的影響機會增加。有關雲端運算資訊安全的確保方式，包含透過技術、管理，以及部分法律規範，有關法律規範，各國立法方式不同，我國係透過民法、刑法、電子簽章法、電信法等不同法律，共同規範資訊安全相關責任，同時嚇阻第三人侵害使用者或服務提供者之系統與資訊。

資訊安全風險無法被完全消除。倘若剩餘之風險實現，則需靠契約分配其承擔損害的範圍。契約亦有分配雙方維護資訊安全責任之功能。

三、 針對貿易雲端契約中之責任分配

因目前立法不及科技發展，相關的法律問題暫時須靠契約解決。在訂契約時，貿易商應對雲端運算的資訊存取與處理模式有所認識，並且瞭解服務提供者提出之契約中，雙方分別的責任為何。

若以對資訊與服務之掌握程度為分配責任依據，使用者與服務提供者在不同服務模式下，其對資訊安全之維護責任有不同負擔。在 SaaS 與 PaaS 模式下，因服務提供者掌握大多數資訊與服務，且從使用者角度，其資訊之控制情形或方法

不完全透明，是以服務提供者應該負擔較大的資訊安全維護責任。在 IaaS 模式時，因服務提供者的服務內容為基礎設施服務，換言之，服務提供者負責維護硬體設備，使用者需自行維護虛擬軟體之資訊安全。

參考 Google、Salesforce、Microsoft、IBM 與 Amazon 既有的雲端服務契約，可發現這些契約就其模式之不同，對維護資訊安全義務的分配權重不相同。Google、Salesforce 與 Microsoft 的服務主要為 SaaS 與 PaaS 服務，服務提供者負擔較大資訊安全維護責任，使用者則負責管理其內部人員與其提供之對象皆遵守條款。IBM Smart Business Cloud 與 Amazon，則因提供的服務包含 SaaS、PaaS 與 IaaS 模式服務，IBM 不對使用者的任何資訊負責。此外，這些雲端運算服務定型化契約中，皆以免責條款、不可抗力條款與有限責任條款排除一方或雙方的部分責任，或是控制損害賠償請求權得以請求之金額，此舉對使用者而言，具有許多不利益，且其是否合理或公平，有待商榷。貿易商在締約時，應注意契約所適用的準據法規定，倘若該準據法不絕對禁止這些條款，這些責任條款仍可能有效，使貿易商負擔潛在的不利益。

我國傳統模式下之資訊業者與客戶，其所訂定的契約與前述雲端運算服務定型化契約相似，或者較為簡陋，然而以這二種契約之對象與複雜程度，適用於傳統模式的契約條款不一定適合雲端運算契約。

第二節　評論與建議

本研究係以貿易商之立場，檢視導入貿易雲端後，所可能面臨的資訊安全風險。經過觀察與比較後，本文歸納出之建議為貿易商重視與雲端運算服務提供者之間的締約。貿易商在導入雲端運算時，應對資訊安全風險與相關因應的技術及管理有所認識，自不待言，但貿易商的資訊既然被存在服務提供者一方，其所能透過技術與管理的直接控制受到極大侷限性，甚至不可能達到，因此透過間接的

方式，亦即以契約保障資訊受到充分完善的管理及保護，是比較實際的做法。

須注意者是，雲端運算服務提供者通常提出一定型化契約，當中除規範雙方須履行的義務與遵守的條款事項外，多半還立有幾個責任條款，透過責任條款分配損害發生時應由誰承擔後果。依第四章之比較，可知雲端運算服務提供者通常以責任條款排除許多責任，並且就剩餘可歸責事項為有限賠償金額之限制，這些規定有礙於使用者在損害發生時主張其權利、填補其損失。

有關前述之責任條款，貿易商應注意該等責任條款在契約約定準據法之下是否為有效，倘若這些責任條款為有效，則應嘗試與服務提供者為協商，盡可能修改這些條款內容，以保障自己的安全。然而，在現實情況中，因雲端服務提供者通常規模較大，而我國個別貿易商多為中小型企業，似難以要求與雲端服務提供者就契約為另外之協議。若貿易商無法改變契約條款內容，則應多比較各個雲端運算服務提供者責任條款之內容。

參考文獻

一、　中文部分

1. William Stalling 著，電腦網路　網際網路協定與技術，王金龍等譯，2006 年 1 月。
2. 王澤鑑，侵權行為法（1）－一般侵權行為，2006 年 8 月初版。
3. 台北市進出口商業同業公會,「2007 年貿易業經營環境調查報告」，2007 年。
4. 台灣經貿網，台灣經貿網供應商會員合約。
5. 行政院主計處，行政院主計處電腦硬體設備採購參考合約。
6. 行政院主計處，行政院主計處電腦硬體設備租賃參考合約。
7. 行政院主計處，行政院主計處電腦硬體設備維護參考合約。
8. 行政院主計處，行政院主計處電腦軟體授權使用參考合約。
9. 行政院主計處，行政院主計處電腦軟體委託開發參考合約。
10. 宋佩珊，個人醫療資訊隱私權保護之立法趨勢探究－以美國、加拿大為例，科技法律透析，2010 年 5 月。
11. 拓墣產業研究所，探索雲端運算市場新商機， 2010 年 7 月。
12. 邱聰智，新訂民法債編通則（下），2003 年 3 月新訂一版。
13. 高大宇等人，資訊安全，2003 年。
14. 張乃文，雲端運算產業發展之策略規劃與法制因應，科技透析法律，2010 年 12 月。
15. 張錦源，國際貿易實務詳論， 2009 年 8 月 14 版。
16. 張錦源、康蕙芬，國際貿易實務，2006 年 10 月 6 版。
17. 黃仲夫，刑法精義，2006 年。
18. 最高法院，最高法院 91 年度台再字第 45 號判決。
19. 最高法院，最高法院 91 年度台上字第 2220 號判決。

20. 彭開英，日韓電子商務法制環境與發展之比較，科技法律透析，2008 年 3 月。
21. 經濟部商業司，2010 中華民國電子商務年鑑。
22. 經濟部國際貿易局電子商務小組，貿易便捷化計畫執行成效與展望，2010 年 11 月 5 日。
23. 蔡孟佳，國際貿易實務， 2006 年 7 月 3 版。
24. 趨勢科技研究：43%的受訪企業曾經遇到雲端服務廠商發生資訊安全問題，自由時報電子版，2011 年 6 月 14 日。
25. 關貿網路，關貿網路使用規範。
26. 露天拍賣，露天會員拍賣合約。

二、 英文部分

1. Armbrust, Michael et al, *A View of Cloud Computing*, Communications of the ACM Vol. 53 No.4 (2010).
2. Armbrust, Michael et al, *Above The Clouds: A Berkeley View Of Cloud Computing*, Technical Report No. UCB/EECS-2009-28, University of California at Berkeley (2009).
3. Brotby, Krag, INFORMATION SECURITY GOVERNANCE (2009).
4. Clarke, Roger, *User Requirements for Cloud Computing Architecture*, 2010 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing (2010).
5. European Network and Information Security Agency, Cloud Computing: Benefits, Risks and Recommendations for Information Security (2009).
6. European Network and Information Security Agency, Cloud Computing Information Assurance Framework (2009).

7. Gilbert, Francoise, *Domain 3: Legal*, *in* Security Guidance for Critical Areas of Focus in Cloud Computing (Cloud Security Alliance ed., 2009).
8. Google, Google Apps for Business Online Agreement.
9. IBM, IBM Smart Business Cloud Agreement.
10. International Organization for Standardization, ISO Risk Management- Principles and Guidelines (ISO 31000: 2009(E)).
11. Mather, Tim et al., CLOUD SECURITY AND PRIVACY (2009).
12. Mell, Peter & Timothy Grance, The NIST Definition Of Cloud Computing (Draft), NIST Special Publication 800-145 (Jan., 2011).
13. Microsoft, Windows Azure Platform Consumption Online Subscription Agreement.
14. Pawluk, Jean, *Domain 14: Storage*, *in* Security Guidance for Critical Areas of Focus in Cloud Computing (Cloud Security Alliance ed, 2009).
15. Paquette, Scott et al., *Identifying the Security Risks Associated with Governmental Use of Cloud Computing*, Government Information Quarterly (2010).
16. Reavis, Jim et al., *Domain 9: Data Center Operations, in* Security Guidance for Critical Areas of Focus in Cloud Computing (Cloud Security Alliance ed., 2009).
17. Reich, Jeffrey N., *Domain 6: Information Lifecycle Management*, *in* Security Guidance for Critical Areas of Focus in Cloud Computing (Cloud Security Alliance ed., 2009).
18. Spivey, Jeff et al., *Domain 8: Traditional Security, Business Continuity and Disaster Recover*, *in* Security Guidance for Critical Areas of Focus in Cloud Computing 55, 55-56 (Cloud Security Alliance ed., 2009).
19. Salesforce, Master Subscription Agreement.
20. Salesforce, Master Subscription Agreement Developer Services.

三、 網路資料

1. 台灣經貿網官方網站，http://www.taiwantrade.com.tw/CH/
2. 行政院主計處，中華民國行業標準分類第 7 次修訂（2001 年 1 月），中華民國統計資訊網，網址：http://www.dgbas.gov.tw/ct.asp?xItem=2203&ctNode=3374
3. 行政院主計處，中華民國台灣地區國民所得統計摘要，中華民國統計資訊網，網址：http://www.stat.gov.tw/ct.asp?xItem=15060&ctNode=3536 台灣綜合研究院，中小企業基本知識，台灣綜合研究院，網址：http://www.tri.org.tw/ceo/。
4. 財政部關稅總局，財政部關稅總局發布 99 年第 4 季與 99 年全年度各項業務統計資料，財政部關稅總局，網址：http://web.customs.gov.tw/ct.asp?xItem=50595&ctNode=12661
5. 經濟部國際貿易局，貿易便捷化簡介，網址：http://cweb.trade.gov.tw/kmi.asp?xdurl=kmif.asp&cat=CAT605
6. 關貿網路官方網站，網址：http://www.tradevan.com.tw/web/guest/home
7. Google 官方網站，網址：http://www.google.com.tw/
8. IBM 官方網站，網址：http://www.ibm.com/us/en/
9. Microsoft 官方網站，網址：http://www.microsoft.com/en-us/default.aspx
10. Salesforce 官方網站，網址：http://www.salesforce.com/tw/?ir=1
11. Wikipedia，網址：http://en.wikipedia.org.

附件一：介宏資訊有限公司　訪談記錄

受訪者：孫元順先生（介宏資訊業務部經理）

受訪時間：2011 年 7 月 15 日上午 9:40

以下分別對介宏資訊產品內容、契約中有關雙方責任分配之相關事項、以及其他訪談內容為記錄。

（一）　介宏資訊產品內容與提供模式

1. 介宏資訊（以下簡稱「介宏」）主要提供與物流業活動相關的系統與平台（以下統稱「產品」），客戶可在單一主機上使用，或透過網路平台，以取得、使用產品內容。
2. 部分產品係由私有雲端模式提供。在此所指的「雲端」，係指網路平台，雲端運算則為在網際網路環境中、透過網際網路功能來處理資訊或儲存資訊。依網路平台的大小，可將雲端區分為私雲、公雲、大公雲、超級雲等類型；又，依網路平台存放地點，若其由客戶自行保有，性質上屬於私雲，若平台在企業外部，其他使用者亦可取得或使用，則為公雲。
3. 有關資訊的處理與儲存，介宏產品具有處理資訊的功能，但無儲存資訊的功能。因此客戶的資訊由客戶自行持有與維護。
4. 因使用介宏產品導致的資訊毀損或滅失，由介宏負責修復。

（二）　介宏資訊交易模式

1. 與個別客戶訂定契約。
2. 契約類型：
   (1) 產品買賣契約：與一般買賣契約無異；
   (2) 維護契約等：若客戶希望增加額外服務，譬如維修、資訊安全維護等，則雙方另訂維護契約或其他服務契約。

（三） 產品之保固與維修

1. 介宏在約定的保固期限內，負責維修產品。
2. 介宏依維護契約的服務內容，負責維修產品。
3. 實際情況中，介宏原則上可遠距離地、即時地解決客戶產品問題，若須到場維修，通常原因是病毒、蠕蟲或其他重大事件，導致系統無法使用，此時大多數客戶對系統問題具有損害嚴重的認知與心理準備。

（四） 介宏的責任範圍與損害賠償限制

1. 介宏與客戶之間的契約條款中，多半沒有訂立免責條款。
2. 介宏對負擔有限的損害賠償責任，損害賠償的上限金額通常依下列兩種方式決定：
   (1) 維護契約中介宏資訊取得的服務報酬；或
   (2) 和客戶另行協議。
3. 若客戶提出無限責任之要求，介宏應該不會選擇締結契約。

（五） 其他訪談內容

1. 因產品、客戶狀況單純，契約的結構不太複雜，大致上規定雙方義務、

產品使用期限、付款方式、管轄法院等。

2. 介宏目前尚未與客戶發生過訴訟。
3. 介宏透過盡量協助客戶解決問題，維護其與客戶間的關係。
4. 介宏在未來發展中，可能朝向公雲發展。在公雲的架構下，介宏與客戶之間的法律關係，將因公雲的性質而呈現比目前更複雜的情況，譬如有主導該公雲的廠商介入。有關公雲相關的法律問題或評估，現行中尚未著手擬訂。

附件二：關貿網路股份有限公司　訪談記錄

受訪者：魏垚德先生（關貿網路股份有限公司稽核室總稽核）

受訪時間：2011 年 7 月 19 日上午 10:30

訪談中與貿易業電子化服務及雲端服務、以及資訊安全相關的記錄如下：

（一） 關貿網路與進出口貿易商及通關的相關服務

1. 有關關貿網路提供給進出口貿易商的服務：

   多屬於加值型的服務。進出口貿易商授權關貿網路去處理他們的資料，譬如資料彙整、將文件格式調整成他們內部使用的格式，以供這些進出口貿易商未來內部使用，譬如 XX 公司去年有一千筆進出口交易，使用關貿網路的服務處理這些資料，關貿網路便將這些資訊彙總起來，製作成 XX 公司要求的文件，XX 公司取得之後，可能供他們內部其他處理用途，比方說將資料直接匯入 ERP（Enterprise Resource Planning，企業資源規劃系統），或供財務之類使用。

2. 有關通關部分服務：

   通關部分的服務，進出口商多半交給報關行處理。進出口商提供給報關行的資料，通常都依照他們自己便利的各種電子格式或書面，報關行再將交付文件的格式轉換為標準訊息，再經由關貿網路將訊息傳送給海關。

（二） 與關貿網路處理完的資訊，其處置與保存事項

1. 關貿網路將處理完的資訊交給進出口商。
2. 關貿網路目前沒有提供資訊儲存的服務,但在未來發展雲端產業時,有構想提供資訊儲存的服務。

(三) 有關文件處理時受到毀損,以及受到毀損後衍生的損害賠償

1. 關貿網路在處理資訊時會備份,或者透過異地備援等方式保存資訊,因此資訊毀損時仍可修復。
2. 資料受到毀損時,依關貿網路使用規範條款,對該毀損負擔修復的責任,但沒有另外負損害賠償。關貿網路通常會及時修復。
3. 會有損害賠償發生,是因資訊在需要被使用時剛好遇到系統故障,導致客戶在那段時間內無法使用資訊。譬如在通關時需要提出文件,但系統當時剛好故障,導致通關作業拖延,此時關貿網路依據網路使用者規範,在構成該規範第 9 條第 2 項的情況下,負擔損害賠償責任。
4. 目前關貿網路尚未遇過前述問題,亦無因資訊毀損等狀況發生過訴訟。

(四) 關貿網路未來發展雲端的可能模式

1. SaaS、PaaS、IaaS 服務模式皆會提供。
2. 與其他軟體公司該如何合作,仍須視業界討論與相互配合的結果。

(五) 關貿網路發展雲端過程中,目前面臨的困難

1. 目前尚未發現新的獲利營運模式。
2. 雲端發展成功與否,與雲端上所放的服務是否為好的服務相關,在目

前，關貿網路仍在思考有哪些服務適合放上雲端。

3. 就目前我國雲端產業市場,比較談到雲端運算的業者為電信業或硬體產業，電信業提供的雲端服務多為 B2C 模式，還沒有聽說 B2B 的模式出現；硬體則可能是提供給國外，亦即 IaaS 模式，譬如現在有廠商製作貨櫃雲，即是把伺服器放至在貨櫃中，給與其通風、電力等環境控制所需的條件，再把這個貨櫃做為一個硬體設備提供給他人。

（六） 關貿網路在幫助企業導入電子商務時，如何消除其對資訊安全的疑慮

1. 本身做好內外的防護措施。內部設備皆受到完善的保護，譬如定期掃毒偵測、配合機制弱點掃描；內控制度有很完善的管理，譬如限制存取資料之人，授權不同人士接觸不同資料。
2. 實務上參考 ISO27001（ISMS）等規範，關貿網路亦採用此一國際標準，包含密碼設定要求、密碼長度設定、定其掃描等事項，ISO27001 中設有規範。
3. 使用關貿網路的企業，其本身是否做好資訊安全，由企業自行負責。

附件三：Googe Apps for Business Online Agreement 部分條款內容

僅節錄本研究討論之條款內容。本條款最後瀏覽日期為 2011 年 11 月 27 日。

Google Apps for Business Online Agreement

This Google Apps for Business Online Agreement (the "Agreement") is entered into by and between Google Inc., a Delaware corporation, with offices at 1600 Amphitheatre Parkway, Mountain View, California 94043 ("Google") and the entity agreeing to these terms ("Customer"). This Agreement is effective as of the date you click the "I Accept" button below (the "Effective Date"). If you are accepting on behalf of your employer or another entity, you represent and warrant that: (i) you have full legal authority to bind your employer, or the applicable entity, to these terms and conditions; (ii) you have read and understand this Agreement; and (iii) you agree, on behalf of the party that you represent, to this Agreement. If you don't have the legal authority to bind your employer or the applicable entity, please do not click the "I Accept" button below. This Agreement governs Customer's access to and use of the Services.

1. Services.

1.1 Facilities and Data Transfer. All facilities used to store and process Customer Data will adhere to reasonable security standards no less protective than the security standards at facilities where Google stores and processes its own information of a similar type. Google has implemented at least industry standard systems and procedures to ensure the security and confidentiality of Customer Data, protect against anticipated threats or hazards to the security or integrity of Customer Data, and protect against unauthorized access to or use of Customer Data.As part of providing the Services, Google may transfer, store and process Customer Data in the United States or any other country in which Google or its agents maintain facilities. By using the Services, Customer consents to this transfer, processing and storage of Customer Data.

2. Customer Obligations.

2.1 Compliance. Customer will use the Services in accordance with the Acceptable Use Policy. Google may make new applications, features or functionality available from time to time through the Services, the use of which may be contingent upon Customer's agreement to additional terms. Customer agrees that its use of the Domain

Service is subject to its compliance with the Domain Service Terms.

2.2 Aliases. Customer is solely responsible for monitoring, responding to, and otherwise processing emails sent to the "abuse" and "postmaster" aliases for Customer Domain Names, but Google may monitor emails sent to these aliases for Customer Domain Names to allow Google to identify Services abuse.

2.3 Customer Administration of the Services. Customer may specify one or more Administrators through the Admin Console who will have the rights to access Admin Account(s) and to administer the End User Accounts. Customer is responsible for: (a) maintaining the confidentiality of the password and Admin Account(s); (b) designating those individuals who are authorized to access the Admin Account(s); and (c) ensuring that all activities that occur in connection with the Admin Account(s) comply with the Agreement. Customer agrees that Google's responsibilities do not extend to the internal management or administration of the Services for Customer and that Google is merely a data-processor.

2.5 Unauthorized Use. Customer will use commercially reasonable efforts to prevent unauthorized use of the Services, and to terminate any unauthorized use. Customer will promptly notify Google of any unauthorized use of, or access to, the Services of which it becomes aware.

2.6 Restrictions on Use. Unless Google specifically agrees in writing, Customer will not, and will use commercially reasonable efforts to make sure a third party does not: (a) sell, resell, lease or the functional equivalent, the Services to a third party (unless expressly authorized in this Agreement); (b) attempt to reverse engineer the Services or any component; (c) attempt to create a substitute or similar service through use of, or access to, the Services; (d) use the Services for High Risk Activities; or (e) use the Services to store or transfer any Customer Data that is controlled for export under Export Control Laws.

5. Suspension.

5.2 Emergency Security Issues. Notwithstanding the foregoing, if there is an Emergency Security Issue, then Google may automatically Suspend the offending use. Suspension will be to the minimum extent and of the minimum duration required to prevent or terminate the Emergency Security Issue. If Google Suspends an End User Account for any reason without prior notice to Customer, at Customer's request, Google will provide Customer the reason for the Suspension as soon as is reasonably possible.

9. Representations, Warranties and Disclaimers.

9.1 Representations and Warranties. Each party represents that it has full power and

authority to enter into the Agreement. Each party warrants that it will comply with all laws and regulations applicable to its provision, or use, of the Services, as applicable (including applicable security breach notification law). Google warrants that it will provide the Services in accordance with the applicable SLA.

9.2 Disclaimers. TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, EXCEPT AS EXPRESSLY PROVIDED FOR HEREIN, NEITHER PARTY MAKES ANY OTHER WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING WITHOUT LIMITATION WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR USE AND NONINFRINGEMENT. GOOGLE MAKES NO REPRESENTATIONS ABOUT ANY CONTENT OR INFORMATION MADE ACCESSIBLE BY OR THROUGH THE SERVICES. CUSTOMER ACKNOWLEDGES THAT THE SERVICES ARE NOT A TELEPHONY SERVICE AND THAT THE SERVICES ARE NOT CAPABLE OF PLACING OR RECEIVING ANY CALLS, INCLUDING EMERGENCY SERVICES CALLS, OVER PUBLICLY SWITCHED TELEPHONE NETWORKS.

11. Termination.

11.2 Effects of Termination. 11.2 If this Agreement terminates, then: (i) the rights granted by one party to the other will cease immediately (except as set forth in this Section); (ii) Google will provide Customer access to, and the ability to export, the Customer Data for a commercially reasonable period of time at Google's then-current rates for the applicable Services; (iii) after a commercially reasonable period of time, Google will delete Customer Data by removing pointers to it on Google's active and replication servers and overwriting it over time; and (iv) upon request each party will promptly use commercially reasonable efforts to return or destroy all other Confidential Information of the other party. If a Customer on an annual plan terminates the Agreement prior to the conclusion of its annual plan, Google will bill Customer, and Customer is responsible for paying Google, for the remaining unpaid amount of Customer’s annual commitment.

13. Limitation of Liability.

13.1 Limitation on Indirect Liability. NEITHER PARTY WILL BE LIABLE UNDER THIS AGREEMENT FOR LOST REVENUES OR INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY, OR PUNITIVE DAMAGES, EVEN IF THE PARTY KNEW OR SHOULD HAVE KNOWN THAT SUCH DAMAGES WERE POSSIBLE AND EVEN IF DIRECT DAMAGES DO NOT SATISFY A REMEDY.

13.2 Limitation on Amount of Liability. NEITHER PARTY MAY BE HELD LIABLE UNDER THIS AGREEMENT FOR MORE THAN THE AMOUNT PAID BY CUSTOMER TO GOOGLE HEREUNDER DURING THE TWELVE MONTHS PRIOR TO THE EVENT GIVING RISE TO LIABILITY.

13.3 Exceptions to Limitations. These limitations of liability apply to the fullest extent permitted by applicable law but do not apply to breaches of confidentiality obligations, violations of a party's Intellectual Property Rights by the other party, or indemnification obligations.

14. Miscellaneous.

14.4 Force Majeure. Neither party will be liable for inadequate performance to the extent caused by a condition (for example, natural disaster, act of war or terrorism, riot, labor condition, governmental action, and Internet disturbance) that was beyond the party's reasonable control.

附件四：Salesforce 部分條款內容

僅節錄本研究討論之條款內容。

I. Master Subscription Agreement

THIS MASTER SUBSCRIPTION AGREEMENT ("AGREEMENT") GOVERNS YOUR ACQUISITION AND USE OF OUR SERVICES.
IF YOU REGISTER FOR A FREE TRIAL FOR OUR SERVICES, THIS AGREEMENT WILL ALSO GOVERN THAT FREE TRIAL.
BY ACCEPTING THIS AGREEMENT, EITHER BY CLICKING A BOX INDICATING YOUR ACCEPTANCE OR BY EXECUTING AN ORDER FORM THAT REFERENCES THIS AGREEMENT, YOU AGREE TO THE TERMS OF THIS AGREEMENT. IF YOU ARE ENTERING INTO THIS AGREEMENT ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY AND ITS AFFILIATES TO THESE TERMS AND CONDITIONS, IN WHICH CASE THE TERMS "YOU" OR "YOUR" SHALL REFER TO SUCH ENTITY AND ITS AFFILIATES. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT AGREE WITH THESE TERMS AND CONDITIONS, YOU MUST NOT ACCEPT THIS AGREEMENT AND MAY NOT USE THE SERVICES.

You may not access the Services if You are Our direct competitor, except with Our prior written consent. In addition, You may not access the Services for purposes of monitoring their availability, performance or functionality, or for any other benchmarking or competitive purposes.
This Agreement was last updated on September 15, 2011. It is effective between You and Us as of the date of You accepting this Agreement.

4. USE OF THE SERVICES
4.1. Our Responsibilities. We shall: (i) provide Our basic support for the Purchased Services to You at no additional charge, and/or upgraded support if purchased separately, (ii) use commercially reasonable efforts to make the Purchased Services available 24 hours a day, 7 days a week, except for: (a) planned downtime (of which We shall give at least 8 hours notice via the Purchased Services and which We shall schedule to the extent practicable during the weekend hours from 6:00 p.m. Friday to

3:00 a.m. Monday Pacific Time), or (b) any unavailability caused by circumstances beyond Our reasonable control, including without limitation, acts of God, acts of government, floods, fires, earthquakes, civil unrest, acts of terror, strikes or other labor problems (other than those involving Our employees), Internet service provider failures or delays, or denial of service attacks, and (iii) provide the Purchased Services only in accordance with applicable laws and government regulations.

4.2. Our Protection of Your Data. We shall maintain appropriate administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Your Data. We shall not (a) modify Your Data, (b) disclose Your Data except as compelled by law in accordance with Section 8.3 (Compelled Disclosure) or as expressly permitted in writing by You, or (c) access Your Data except to provide the Services and prevent or address service or technical problems, or at Your request in connection with customer support matters.

4.3. Your Responsibilities. You shall (i) be responsible for Users' compliance with this Agreement, (ii) be responsible for the accuracy, quality and legality of Your Data and of the means by which You acquired Your Data, (iii) use commercially reasonable efforts to prevent unauthorized access to or use of the Services, and notify Us promptly of any such unauthorized access or use, and (iv) use the Services only in accordance with the User Guide and applicable laws and government regulations. You shall not (a) make the Services available to anyone other than Users, (b) sell, resell, rent or lease the Services, (c) use the Services to store or transmit infringing, libelous, or otherwise unlawful or tortious material, or to store or transmit material in violation of third-party privacy rights, (d) use the Services to store or transmit Malicious Code, (e) interfere with or disrupt the integrity or performance of the Services or third-party data contained therein, or (f) attempt to gain unauthorized access to the Services or their related systems or networks.

8. CONFIDENTIALITY

8.1. Definition of Confidential Information. As used herein, "Confidential Information" means all confidential information disclosed by a party ("Disclosing Party") to the other party ("Receiving Party"), whether orally or in writing, that is designated as confidential or that reasonably should be understood to be confidential given the nature of the information and the circumstances of disclosure. Your Confidential Information shall include Your Data; Our Confidential Information shall include the Services; and Confidential Information of each party shall include the terms and conditions of this Agreement and all Order Forms, as well as business and marketing plans, technology and technical information, product plans and designs, and business processes disclosed by such party. However, Confidential Information

(other than Your Data) shall not include any information that (i) is or becomes generally known to the public without breach of any obligation owed to the Disclosing Party, (ii) was known to the Receiving Party prior to its disclosure by the Disclosing Party without breach of any obligation owed to the Disclosing Party, (iii) is received from a third party without breach of any obligation owed to the Disclosing Party, or (iv) was independently developed by the Receiving Party.

8.2. Protection of Confidential Information. The Receiving Party shall use the same degree of care that it uses to protect the confidentiality of its own confidential information of like kind (but in no event less than reasonable care) (i) not to use any Confidential Information of the Disclosing Party for any purpose outside the scope of this Agreement, and (ii) except as otherwise authorized by the Disclosing Party in writing, to limit access to Confidential Information of the Disclosing Party to those of its and its Affiliates' employees, contractors and agents who need such access for purposes consistent with this Agreement and who have signed confidentiality agreements with the Receiving Party containing protections no less stringent than those herein. Neither party shall disclose the terms of this Agreement or any Order Form to any third party other than its Affiliates and their legal counsel and accountants without the other party's prior written consent.

9. WARRANTIES AND DISCLAIMERS

9.1. Our Warranties. We warrant that (i) We have validly entered into this Agreement and have the legal power to do so, (ii) the Services shall perform materially in accordance with the User Guide, (iii) subject to Section 5.3 (Integration with Non-Salesforce.com Services), the functionality of the Services will not be materially decreased during a subscription term, and (iv) We will not transmit Malicious Code to You, provided it is not a breach of this subpart (v) if You or a User uploads a file containing Malicious Code into the Services and later downloads that file containing Malicious Code. For any breach of a warranty above, Your exclusive remedy shall be as provided in Section 12.3 (Termination for Cause) and Section 12.4 (Refund or Payment upon Termination) below.

9.2. Your Warranties. You warrant that You have validly entered into this Agreement and have the legal power to do so.

9.3. Disclaimer. EXCEPT AS EXPRESSLY PROVIDED HEREIN, NEITHER PARTY MAKES ANY WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, AND EACH PARTY SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW.

11. LIMITATION OF LIABILITY

11.1. Limitation of Liability. NEITHER PARTY'S LIABILITY WITH RESPECT TO ANY SINGLE INCIDENT ARISING OUT OF OR RELATED TO THIS AGREEMENT (WHETHER IN CONTRACT OR TORT OR UNDER ANY OTHER THEORY OF LIABILITY) SHALL EXCEED THE LESSER OF $500,000 OR THE AMOUNT PAID BY YOU HEREUNDER IN THE 12 MONTHS PRECEDING THE INCIDENT, PROVIDED THAT IN NO EVENT SHALL EITHER PARTY'S AGGREGATE LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT (WHETHER IN CONTRACT OR TORT OR UNDER ANY OTHER THEORY OF LIABILITY) EXCEED THE TOTAL AMOUNT PAID BY YOU HEREUNDER. THE FOREGOING SHALL NOT LIMIT YOUR PAYMENT OBLIGATIONS UNDER SECTION 6 (FEES AND PAYMENT FOR PURCHASED SERVICES).

11.2. Exclusion of Consequential and Related Damages. IN NO EVENT SHALL EITHER PARTY HAVE ANY LIABILITY TO THE OTHER PARTY FOR ANY LOST PROFITS OR REVENUES OR FOR ANY INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, COVER OR PUNITIVE DAMAGES HOWEVER CAUSED, WHETHER IN CONTRACT, TORT OR UNDER ANY OTHER THEORY OF LIABILITY, AND WHETHER OR NOT THE PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE FOREGOING DISCLAIMER SHALL NOT APPLY TO THE EXTENT PROHIBITED BY APPLICABLE LAW.

12. TERM AND TERMINATION

12.4. Refund or Payment upon Termination. Upon any termination for cause by You, We shall refund You any prepaid fees covering the remainder of the term of all subscriptions after the effective date of termination. Upon any termination for cause by Us, You shall pay any unpaid fees covering the remainder of the term of all Order Forms after the effective date of termination. In no event shall any termination relieve You of the obligation to pay any fees payable to Us for the period prior to the effective date of termination.

12.5. Return of Your Data. Upon request by You made within 30 days after the effective date of termination of a Purchased Services subscription, We will make available to You for download a file of Your Data in comma separated value (.csv) format along with attachments in their native format. After such 30-day period, We shall have no obligation to maintain or provide any of Your Data and shall thereafter, unless legally prohibited, delete all of Your Data in Our systems or otherwise in Our possession or under Our control.

II. Master Subscription Agreement Developer Service

This Master Subscription Agreement (“Agreement”) is for Your use of the Developer Services to develop and maintain applications and services that interoperate with or complement Our online platform and/or applications.

YOU INDICATE YOUR ACCEPTANCE OF THIS AGREEMENT BY CLICKING A CHECK BOX OR BUTTON OR EXECUTING AN ORDER FORM THAT REFERENCES THIS AGREEMENT, OR BY ACCESSING THE DEVELOPER SERVICES. BY ACCEPTING THIS AGREEMENT, YOU AGREE TO ITS TERMS. IF YOU ARE ENTERING INTO THIS AGREEMENT ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY AND ITS AFFILIATES TO THESE TERMS AND CONDITIONS, IN WHICH CASE THE TERMS "YOU" OR "YOUR" SHALL REFER TO SUCH ENTITY AND ITS AFFILIATES. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT AGREE WITH THESE TERMS AND CONDITIONS, YOU MUST NOT ACCEPT THIS AGREEMENT AND MAY NOT USE THE DEVELOPER SERVICES.

You may not, without our prior written consent, access or use the Developer Services:

• for production purposes, or

• if You are Our direct competitor, or

• to monitor the availability, performance or functionality of the Developer Services, or

• for any other benchmarking or competitive purposes.

This Agreement was last updated on October 25, 2010. It is effective between You and Us as of the date of You accept this Agreement.

2. PROVISION AND USE OF DEVELOPER SERVICES

2.3. Our Responsibilities. We shall use commercially reasonable efforts to: (i) make the Developer Services available 24 hours a day, 7 days a week, except for: (a) planned downtime (of which We shall give at least 8 hours notice via the Developer Services and which We shall schedule to the extent practicable during the weekend hours from 6:00 p.m. Pacific time Friday to 3:00 a.m. Pacific time Monday), or (b) any unavailability caused by circumstances beyond Our reasonable control, including without limitation, acts of God, acts of government, flood, fire, earthquakes, civil unrest, acts of terror, strikes or other labor problems (other than those involving Our employees), or Internet service provider failures or delays, and (ii) provide the Developer Services in accordance with applicable laws and government regulations.

The Basic Developer Services exclude support. We may make developer support available separately as a Supplemental Developer Service or through other programs from time to time.

2.4. Your Responsibilities. You shall (i) be responsible for Users' compliance with this Agreement, (ii) be solely responsible for the accuracy, quality, integrity and legality of Your Data and of the means by which You acquired Your Data, (iii) use commercially reasonable efforts to prevent unauthorized access to or use of the Developer Services, and notify Us promptly of any such unauthorized access or use, and (iv) use the Developer Services only in accordance with the User Guide and applicable laws and government regulations. You shall not (a) make the Developer Services available to any person or entity other than Users, (b) sell, resell, rent or lease the Developer Services, (c) use the Developer Services to store or transmit infringing, libelous, or otherwise unlawful or tortious material, or to store or transmit material in violation of third-party privacy or confidentiality rights, (d) use the Developer Services to store or transmit Malicious Code, (e) interfere with or disrupt the integrity or performance of the Developer Services or third-party data contained therein, or (f) attempt to gain unauthorized access to the Developer Services or their related systems or networks.

6. CONFIDENTIALITY

6.1. Definition of Confidential Information. As used herein, "Confidential Information" means, in the case of information disclosed by Us to You, the Developer Services; and in the case of information disclosed by You to Us, Your Data, and information regarding applications or other materials developed using the Developer Services to the extent disclosed to Us by the hosting of such applications or materials on our platform or to the extent disclosed to our Customer Support organization. However, Confidential Information shall not include any information that (i) is or becomes generally known to the public without breach of any obligation owed to the disclosing party (the "Disclosing Party"), (ii) was known to the receiving party (the "Receiving Party") prior to its disclosure by the Disclosing Party without breach of any obligation owed to the Disclosing Party, (iii) is received from a third party without breach of any obligation owed to the Disclosing Party, or (iv) was independently developed by the Receiving Party.

6.2. Protection of Confidential Information. Except as otherwise permitted in writing by the Disclosing Party, (i) the Receiving Party shall use the same degree of care that it uses to protect the confidentiality of its own confidential information of like kind (but in no event less than reasonable care) not to disclose or use any Confidential Information of the Disclosing Party for any purpose outside the scope of this Agreement, and (ii) the Receiving Party shall limit access to Confidential Information

of the Disclosing Party to those of its employees, contractors and agents who need such access for purposes consistent with this Agreement and who have signed confidentiality agreements with the Receiving Party containing protections no less stringent than those herein.

7. LIMITED WARRANTIES AND DISCLAIMERS

Each party represents and warrants that it has the legal power to enter into this Agreement. EXCEPT AS PROVIDED IN THE PRECEDING SENTENCE AND IN SECTION 11.5 (WARRANTIES) BELOW, NEITHER PARTY MAKES IN THIS AGREEMENT ANY WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, AND EACH PARTY SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW.

9. LIMITATION OF LIABILITY

9.1. Limitation of Liability. IN NO EVENT SHALL OUR AGGREGATE LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT, WHETHER IN CONTRACT, TORT OR UNDER ANY OTHER THEORY OF LIABILITY, EXCEED THE TOTAL AMOUNT PAID BY YOU HEREUNDER OR, WITH RESPECT TO ANY SINGLE INCIDENT, THE LESSER OF $500,000 OR THE AMOUNT PAID BY YOU HEREUNDER IN THE 12 MONTHS PRECEDING THE INCIDENT.

9.2. Exclusion of Consequential and Related Damages. IN NO EVENT SHALL WE HAVE ANY LIABILITY TO YOU FOR ANY LOST PROFITS OR REVENUES OR FOR ANY INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, COVER OR PUNITIVE DAMAGES HOWEVER CAUSED, WHETHER IN CONTRACT, TORT OR UNDER ANY OTHER THEORY OF LIABILITY, AND WHETHER OR NOT THE PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE FOREGOING DISCLAIMER SHALL NOT APPLY TO THE EXTENT PROHIBITED BY APPLICABLE LAW.

10. TERM AND TERMINATION

10.4. Return of Your Data. Upon request by You made within 30 days after the effective date of termination of a Developer Services subscription, We will make available to You for download a file of Your Data in comma separated value (.csv) format along with attachments in their native format. After such 30-day period, We shall have no obligation to maintain or provide any of Your Data and shall thereafter,

unless legally prohibited, delete all of Your Data in Our systems or otherwise in Our possession or under Our control.

10.5. Loss of Applications and Materials. UPON ANY TERMINATION OF THIS AGREEMENT, ALL APPLICATIONS AND OTHER MATERIALS DEVELOPED BY YOU USING THE DEVELOPER SERVICES AND HOSTED ON OUR PLATFORM WILL BE PERMANENTLY LOST.

11. ADDITIONAL TERMS APPLICABLE TO SUPPLEMENTAL DEVELOPER SERVICES

11.5. Warranties Regarding Supplemental Developer Services. a. Developer Services. We warrant that (i) the Supplemental Developer Services shall perform materially in accordance with the User Guide, and (ii) subject to Section 3.3 (Developer Service Features that Integrate with Third-Party Services), the functionality of the Supplemental Developer Services will not be materially decreased during a subscription term. For any breach of either such warranty, Your exclusive remedy shall be as provided in Sections 11.7.b (Termination for Cause) and 11.7.c (Refund or Payment upon Termination) below. b. Malicious Code. Each party represents and warrants that it will not transmit to the other party any Malicious Code; provided, however, We will not be deemed to breach this warranty to the extent You or a User upload into the Developer Services a file containing Malicious Code and later download that file.

附件五：Microsoft 之 Online Subscription Agreement 部分條款內容

僅節錄本研究討論之條款內容。本條款最後瀏覽日期為 2011 年 11 月 27 日。

Microsoft Online Subscription Agreement

This Microsoft Online Subscription Agreement is between the entity that accepts this agreement ("you") and Microsoft Operations Pte Ltd. ("us", "we"). This agreement consists of: (1) the below terms and conditions; (2) the Online Services Use Rights; (3) the Service Level Agreements; and (4) the pricing and payment terms available via the Portal. This agreement is effective on the date we provide you with a confirmation for your first Order. You enter into this agreement for business purposes only.

3. Your use of our Products.

a. General. This agreement governs your use of the Products. You may need to activate an Online Service prior to use. We grant you a License to Products you ordered provided you pay for them and comply with this agreement. Your License is non-exclusive, non-perpetual, and, unless specifically allowed, non-transferable. Minimum system requirements or other factors may affect your ability to use Products. We reserve all rights not expressly granted in this agreement.

b. Service Level Agreement. We will provide Online Services according to the Service Level Agreement(s) located at http://www.microsoft.com/licensing/contracts or at an alternate site that we identify.

c. Privacy, Use and Security of Customer Data. We will handle your Customer Data according to the privacy, use and security terms set forth in the Online Services Use Rights.

7. Warranties.

a. Limited warranty. We warrant that:
Online Services will perform in accordance with the Service Level Agreement; and
Licensed Software will perform substantially as described in the applicable Microsoft user documentation.

b. Limited warranty term. The limited warranty for:
Online Services is for the duration of your use of the Online Service; and

Licensed Software is one year from the date you first use it.

c. Limited warranty exclusions. This limited warranty is subject to the following limitations:

i. any implied warranties, guarantees or conditions not able to be disclaimed as a matter of law will last one year from the start of the limited warranty;

ii. this limited warranty does not cover problems caused by accident, abuse or use of the Products in a manner inconsistent with this agreement or the Online Services Use Rights, or resulting from events beyond our reasonable control;

iii. this limited warranty does not apply to problems caused by the failure to meet minimum system requirements; and

iv. this limited warranty does not apply to free, trial, pre-release or beta Products.

d. Remedies for breach of limited warranty. If we fail to meet any of the above limited warranties and you notify us within the warranty period that a Product does not meet the limited warranty, then we will:

i. for Online Services, provide the remedies identified in the Service Level Agreement for the affected Online Service; and

ii. for Licensed Software, at our option either (1) return the price paid or (2) repair or replace the Licensed Software.

These are your only remedies for breach of the limited warranty, unless other remedies are required to be provided under applicable law.

e. DISCLAIMER OF OTHER WARRANTIES. OTHER THAN THIS LIMITED WARRANTY, WE PROVIDE NO OTHER EXPRESS OR IMPLIED WARRANTIES OR CONDITIONS. WE DISCLAIM ANY IMPLIED REPRESENTATIONS, WARRANTIES OR CONDITIONS, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, TITLE OR NON-INFRINGEMENT. THESE DISCLAIMERS WILL APPLY UNLESS APPLICABLE LAW DOES NOT PERMIT THEM.

9. Limitation of liability.

a. Limitation on liability. Except as otherwise provided in this Section, to the extent permitted by applicable law, our and our Affiliates' and contractors' liability to you arising under this agreement is limited to direct damages up to the amount you paid us for the Product giving rise to that liability during the (1) Term or (2) twelve months prior to the filing of the claim, whichever is less. In the case of Products provided free of charge, or any code that you are authorized to redistribute to third parties without separate payment to Microsoft, our and our

Affiliates' and contractors' liability to you arising under this agreement is limited to five United States dollars ($5.00 USD). These limitations apply regardless of whether the liability is based on breach of contract, tort (including negligence), strict liability, breach of warranties, or any other legal theory. However, these monetary limitations will not apply to:

i. Our obligations under the Section titled "Defense of infringement, misappropriation, and third party claims";

ii. liability for damages awarded by a court of final adjudication for our or our employees' or agents' gross negligence or willful misconduct;

iii. liabilities arising out of any breach of our obligations under the Section entitled "Confidentiality", except that our and our Affiliates' and contractors' liability arising out of or in relation to Customer Data shall in all cases be limited to the amount you paid for the Online Service giving rise to that liability during the (1) Term or (2) twelve months prior to the filing of the claim, whichever is less; and

iv. liability for personal injury or death caused by our negligence or that of our employees or agents or for fraudulent misrepresentation.

b. EXCLUSION OF CERTAIN DAMAGES. TO THE EXTENT PERMITTED BY APPLICABLE LAW, WHATEVER THE LEGAL BASIS FOR THE CLAIM, NEITHER PARTY, NOR ANY OF ITS AFFILIATES OR SUPPLIERS, WILL BE LIABLE FOR ANY INDIRECT, CONSEQUENTIAL, SPECIAL OR INCIDENTAL DAMAGES, DAMAGES FOR LOST PROFITS OR REVENUES, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION ARISING IN CONNECTION WITH THIS AGREEMENT, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR IF SUCH POSSIBILITY WAS REASONABLY FORESEEABLE. HOWEVER, THIS EXCLUSION DOES NOT APPLY TO EITHER PARTY'S LIABILITY TO THE OTHER FOR VIOLATION OF ITS CONFIDENTIALITY OBLIGATIONS (EXCEPT TO THE EXTENT THAT SUCH VIOLATION RELATES TO CUSTOMER DATA), THE OTHER PARTY'S INTELLECTUAL PROPERTY RIGHTS, OR THE PARTIES' RESPECTIVE OBLIGATIONS IN THE SECTION TITLED "DEFENSE OF INFRINGEMENT, MISAPPROPRIATION, AND THIRD PARTY CLAIMS."

11. Miscellaneous.

n. Force majeure. Neither party will be liable for any failure in performance due to causes beyond either party's reasonable control (such as fire, explosion, power blackout, earthquake, flood, severe storms, strike, embargo, labor disputes, acts of

civil or military authority, war, terrorism (including cyber terrorism), acts of God, acts or omissions of Internet traffic carriers, actions or omissions of regulatory or governmental bodies (including the passage of laws or regulations or other acts of government that impact the delivery of Online Services)). This Section will not, however, apply to your payment obligations under this agreement.

附錄六：Amazon 之 AWS Customer Agreement 部分條款內容

僅節錄本研究討論之條款內容。

AWS Customer Agreement

Last updated August 23, 2011

This AWS Customer Agreement (this "Agreement") contains the terms and conditions that govern your access to and use of the Service Offerings (as defined below) and is an agreement between Amazon Web Services LLC ("AWS," "we," "us," or "our") and you or the entity you represent ("you"). This Agreement takes effect when you click an "I Accept" button or check box presented with these terms or, if earlier, when you use any of the Service Offerings (the "Effective Date"). You represent to us that you are lawfully able to enter into contracts (e.g., you are not a minor). If you are entering into this Agreement for an entity, such as the company you work for, you represent to us that you have legal authority to bind that entity. Please see Section 14 for definitions of certain capitalized terms used in this Agreement.

1. Use of the Service Offerings.

1.2 Your Account. To access the Services, you must create an AWS account associated with a valid e-mail address. Unless explicitly permitted by the Service Terms, you may only create one account per email address. You are responsible for all activities that occur under your account, regardless of whether the activities are undertaken by you, your employees or a third party (including your contractors or agents) and, except to the extent caused by our breach of this Agreement, we and our affiliates are not responsible for unauthorized access to your account. You will contact us immediately if you believe an unauthorized third party may be using your account or if your account information is lost or stolen. You may terminate your account and this Agreement at any time in accordance with Section 7.

3. Security and Data Privacy.

3.1 AWS Security. Without limiting Section 10 or your obligations under Section 4.2, we will implement reasonable and appropriate measures designed to help you secure Your Content against accidental or unlawful loss, access or disclosure.

3.2 Data Privacy. We participate in the safe harbor programs described in the Privacy Policy. You may specify the AWS regions in which Your Content will be stored and

accessible by End Users. We will not move Your Content from your selected AWS regions without notifying you, unless required to comply with the law or requests of governmental entities. You consent to our collection, use and disclosure of information associated with the Service Offerings in accordance with our Privacy Policy, and to the processing of Your Content in, and the transfer of Your Content into, the AWS regions you select.

4. Your Responsibilities

4.2 Other Security and Backup. You are responsible for properly configuring and using the Service Offerings and taking your own steps to maintain appropriate security, protection and backup of Your Content, which may include the use of encryption technology to protect Your Content from unauthorized access and routine archiving Your Content. AWS log-in credentials and private keys generated by the Services are for your internal use only and you may not sell, transfer or sublicense them to any other entity or person, except that you may disclose your private key to your agents and subcontractors performing work on your behalf.

4.3 End User Violations. You will be deemed to have taken any action that you permit, assist or facilitate any person or entity to take related to this Agreement, Your Content or use of the Service Offerings. You are responsible for End Users' use of Your Content and the Service Offerings. You will ensure that all End Users comply with your obligations under this Agreement and that the terms of your agreement with each End User are consistent with this Agreement. If you become aware of any violation of your obligations under this Agreement by an End User, you will immediately terminate such End User's access to Your Content and the Service Offerings.

7. Term; Termination

7.3. Effect of Termination.

(a) Generally. Upon any termination of this Agreement:

(i) all your rights under this Agreement immediately terminate;

(ii) you remain responsible for all fees and charges you have incurred through the date of termination, including fees and charges for in-process tasks completed after the date of termination;

(iii) you will immediately return or, if instructed by us, destroy all AWS Content in your possession; and

(iv) Sections 4.1, 5.2, 7.3, 8 (except the license granted to you in Section 8.4), 9, 10, 11, 13 and 14 will continue to apply in accordance with their terms.

(b) Post-Termination Assistance. Unless we terminate your use of the Service Offerings pursuant to Section 7.2(b), during the 30 days following termination:

(i) we will not erase any of Your Content as a result of the termination;
(ii) you may retrieve Your Content from the Services only if you have paid any charges for any post-termination use of the Service Offerings and all other amounts due; and
(iii) we will provide you with the same post-termination data retrieval assistance that we generally make available to all customers.
Any additional post-termination assistance from us is subject to mutual agreement by you and us.

10. Disclaimers.

THE SERVICE OFFERINGS ARE PROVIDED "AS IS." WE AND OUR AFFILIATES AND LICENSORS MAKE NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE REGARDING THE SERVICE OFFERINGS OR THE THIRD PARTY CONTENT, INCLUDING ANY WARRANTY THAT THE SERVICE OFFERINGS OR THIRD PARTY CONTENT WILL BE UNINTERRUPTED, ERROR FREE OR FREE OF HARMFUL COMPONENTS, OR THAT ANY CONTENT, INCLUDING YOUR CONTENT OR THE THIRD PARTY CONTENT, WILL BE SECURE OR NOT OTHERWISE LOST OR DAMAGED. EXCEPT TO THE EXTENT PROHIBITED BY LAW, WE AND OUR AFFILIATES AND LICENSORS DISCLAIM ALL WARRANTIES, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR QUIET ENJOYMENT, AND ANY WARRANTIES ARISING OUT OF ANY COURSE OF DEALING OR USAGE OF TRADE.

11. Limitations of Liability.

WE AND OUR AFFILIATES OR LICENSORS WILL NOT BE LIABLE TO YOU FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES (INCLUDING DAMAGES FOR LOSS OF PROFITS, GOODWILL, USE, OR DATA), EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. FURTHER, NEITHER WE NOR ANY OF OUR AFFILIATES OR LICENSORS WILL BE RESPONSIBLE FOR ANY COMPENSATION, REIMBURSEMENT, OR DAMAGES ARISING IN CONNECTION WITH: (A) YOUR INABILITY TO USE THE SERVICES, INCLUDING AS A RESULT OF ANY (I) TERMINATION OR SUSPENSION OF THIS AGREEMENT OR YOUR USE OF OR ACCESS TO THE SERVICE OFFERINGS, (II) OUR DISCONTINUATION OF ANY OR ALL OF THE

SERVICE OFFERINGS, OR, (III) WITHOUT LIMITING ANY OBLIGATIONS UNDER THE SLAS, ANY UNANTICIPATED OR UNSCHEDULED DOWNTIME OF ALL OR A PORTION OF THE SERVICES FOR ANY REASON, INCLUDING AS A RESULT OF POWER OUTAGES, SYSTEM FAILURES OR OTHER INTERRUPTIONS; (B) THE COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; (c) ANY INVESTMENTS, EXPENDITURES, OR COMMITMENTS BY YOU IN CONNECTION WITH THIS AGREEMENT OR YOUR USE OF OR ACCESS TO THE SERVICE OFFERINGS; OR (D) ANY UNAUTHORIZED ACCESS TO, ALTERATION OF, OR THE DELETION, DESTRUCTION, DAMAGE, LOSS OR FAILURE TO STORE ANY OF YOUR CONTENT OR OTHER DATA. IN ANY CASE, OUR AND OUR AFFILIATES' AND LICENSORS' AGGREGATE LIABILITY UNDER THIS AGREEMENT WILL BE LIMITED TO THE AMOUNT YOU ACTUALLY PAY US UNDER THIS AGREEMENT FOR THE SERVICE THAT GAVE RISE TO THE CLAIM DURING THE 12 MONTHS PRECEDING THE CLAIM.

13. Miscellaneous.

13.1 Confidentiality and Publicity. You may use AWS Confidential information only in connection with your use of the Service Offerings as permitted under this Agreement. You will not disclose AWS Confidential Information during the Term or at any time during the 5 year period following the end of the Term. You will take all reasonable measures to avoid disclosure, dissemination or unauthorized use of AWS Confidential Information, including, at a minimum, those measures you take to protect your own confidential information of a similar nature. You will not issue any press release or make any other public communication with respect to this Agreement or your use of the Service Offerings. You will not misrepresent or embellish the relationship between us and you (including by expressing or implying that we support, sponsor, endorse, or contribute to you or your business endeavors), or express or imply any relationship or affiliation between us and you or any other person or entity except as expressly permitted by this Agreement.

13.2 Force Majeure. We and our affiliates will not be liable for any delay or failure to perform any obligation under this Agreement where the delay or failure results from any cause beyond our reasonable control, including acts of God, labor disputes or other industrial disturbances, systemic electrical, telecommunications, or other utility failures, earthquake, storms or other elements of nature, blockages, embargoes, riots, acts or orders of government, acts of terrorism, or war.