/THEORY/IN/PRACTICE

雲端資安與隱私
企業風險應對之道
Cloud Security and Privacy

Tim Mather
Subra Kumaraswamy
Shahed Latif 著
胡為君 譯

REILLY®

雲端資安與隱私

企業風險應對之道

Tim Mather, Subra Kumaraswamy & Shahed Latif 著

胡為君 譯

O'REILLY®

碁峰資訊

國家圖書館出版品預行編目資料

雲端資安與隱私：企業風險應對之道 / 胡為君譯. -- 初版.
-- 臺北市：碁峰資訊, 2012.05
面； 公分
譯自：Cloud Security and Privacy
ISBN 978-986-276-476-3 (平裝)
1.資訊安全 2.網路隱私權
312.76 101005661

書　　名	雲端資安與隱私｜企業風險應對之道
書　　號	A270
譯　　者	胡為君
建議售價	NT$580
發 行 人	廖文良
發 行 所	碁峰資訊股份有限公司
地　　址	台北市南港區三重路 66 號 7 樓之 6
電　　話	(02)2788-2408
傳　　真	(02)2788-1031
法律顧問	明貞法律事務所　胡坤佑律師
版　　次	2012 年 05 月初版

對本書的讚譽

對於許多公司，引入雲端運算，是個必然的策略走向。平價運算、普遍的機動性，以及虛擬化技術帶來的優勢，創造出了更靈活的平台，以及更具成本效益的業務應用程式與IT架構。雲端引領著安全控制領域中廣泛、富創造性的應用發展，也在安全程序與管理方面提出了最佳作法的需求。本書為致力於建立雲端安全的人，提供了指引與協助。本書是雲端運算之旅的絕佳起點。

—*Jerry Archer*，CISO，Intuit

本書廣泛涵蓋了IT與資訊安全人員所需的詞彙與定義。本書也勾勒出基礎，讓IT與資訊安全人員可以有效合作，規劃與實作雲端運算服務。學習雲端運算安全與隱私問題時，本書為必讀。

—*David Hahn*，SVP&Group資訊安全長，Wells Fargo Bank

為瞭解雲端運算、為描述此類技術的相關安全問題，先前已有諸多嘗試。本書是最早深入探索雲端運算定義、探討現今引入此類技術時重大風險相關解決方案的著作之一。

—*David Thompson*，Symante服務集團總裁，Symantec

如今，分散式資訊的使用與管理已經成真。雲端運算為資訊使用的普及，提供了更經濟有效的暴政，但同時也放大了現有的風險，更導入了尚未發現、無從管理的新風險。本書適合每一位有興趣於瞭解雲端運算相關風險與回報，以及希望在新一波資訊管理革命中搶先擬定實用計畫的讀者。

—*Michelle Dennedy*，昇陽電腦管理長，昇陽電腦

前言

2008 年 2 月，我遇見了昇陽電腦的 Subra Kumaraswamy，地點是美國密勤局位於舊金山的電子犯罪特別小組總部。Subra 和我一起參與了許多會議，先前我們早在許多類似的專業場合中互相熟識。我們都是資訊安全從業人員，而我們混了多年的矽谷，可是個很小的圈子。Subra 問我有何計畫，我告訴他，我打算寫一本關於雲端運算與安全的書。

直到 2008 年 2 月，矽谷對於雲端運算的炒作仍甚囂塵上。同樣地，大家對於雲端運算欠缺安全性（或者該說是欠缺知識）仍多有顧慮。當 Subra 與我討論時，關於此課題仍無明確的資訊，而這也是我打算寫此課題的動機。Subra 告訴我，他也花不少時間在研究雲端運算，卻無法找到任何明確的相關資訊。我詢問 Subra 是否願意協助我寫這樣的一本書，他同意了（由於先前經歷過寫書的痛苦，我想找可靠的助力，而 Subra 絕對符合要求）。本書的偉大航道於焉啟程。

原本，我們只打算在另一本 O'Reilly 的雲端運算書籍中撰寫一章。然而我們所寫的篇幅長度，很快就超過了 O'Reilly 對於「章」的標準，勢必得變成兩章，於是我們提出將這個想法變成一本探討雲端安全與隱私的專書。O'Reilly 接受了我們的提案，原本只想寫 20 頁，卻成了 200 頁。在短時間內完成這樣的份量，以期成為市場上第一本此類書籍，工作自然不輕鬆。

2008 年底，Subra 與我開始在矽谷對各種不同的技術人員演講，說明我們在雲端運算與安全方面的發現。我們對於聽眾的反應非常高興。沒有人認為我們在技術方面偏離了市場，聽眾渴求更多的資訊與細節。在其中一場演講結束後，一位 KPMG 的員工表示，希望能和我們深入談論雲端運算與稽核。由於本書還需要更好的素材，Subra 與我欣然同意會面。

這次會面其實不如我們所預期。我們原本以為會從 KPMG 的考量與雲端服務的稽核趨勢，獲得一些資訊。但一位與會者 Shahed Latif 詢問能否參與本書的撰寫。Subra 與我在討論後，同意請他加入。我們需要良好的稽核資訊，而 Shahed 絕對是這方面的權威（除了他豐富的稽核經歷，Shahed 身為 KPMG 的合夥人，這間大型雲端服務供應商提供了許多 Subra 和我熟知的服務，所以我們與這位在雲端服務供應商任職多年的資深資訊安全專家洽談愉快）。此外，我認識了 Shahed。我曾經三度與 KPMG 稽核作業合作密切：分別在 Apple、VeriSign 與 Symantec。事實上，當我於 Symantec 擔任資訊安全長時，Shahed 就是 KPMG 的 IT 稽核合作夥伴。所以，我們對 Shahed 再熟不過。

三位作者都到齊了，我們隨即動手，希望能儘快完成本書，在市場上率先出擊。

— Tim Mather

本書訴求讀者

任何對雲端運算有興趣的人都應閱讀本書。雖然主要是談雲端服務的安全、隱私與稽核，我們並非針對資訊安全專家，雖說我們認為大部分資安專家會認為本書有所幫助。我們撰寫本書，是為了想瞭解技術層面的商務人士，以及想用雲端運算且希望能保護資訊的人。資料是王道，而資料的保密性、完整性與可用性，都比以往更為重要。所以，雲端服務的安全、隱私與稽核，都應當會讓我們的讀者更感興趣。

本書內容

在本書，我們會以系統化的方法定義雲端運算，並檢視此新模型帶來的安全與隱私問題。以下是本書各章摘要：

第 1 章，簡介

介紹雲端運算的概念，以及雲端運算帶來的革命。

第 2 章，何謂雲端運算

把雲端運算定義為下列五項屬性：多用戶（multitenancy，共用資源），高擴充性，高彈性，隨需付費，以及自助式資源。然而，雲端運算這個詞彙有多種定義，因為這是個不斷推陳出新的領域。例如，最新的報告指出，雲端運算有超過 22 種不同的定義。* 在本章，我們探討在雲端運算中最廣為接受的服務類型，因為有一些是很重要的新興技術，如虛擬化（virtualization）。

第 3 章，架構安全

描述雲端服務通常提供的 IT 架構安全能力。IT 架構安全，表示在網路、主機與應用層所建立的安全能力。

第 4 章，資料安全與儲存

探討當前的資料安全性以及雲端上的資料儲存，包括保密性、完整性與可及性。

第 5 章，身份與存取管理

說明身份與存取管理（identity and access management，IAM）方法，以及驗證、授權與稽核雲端服務用戶的支援能力。

第 6 章，雲端安全管理

說明雲端相關的安全管理架構與標準。

第 7 章，隱私

介紹與雲端相關的私密性問題，並分析與傳統運算模式的相近與相異之處。此外在本章，我們會著重與雲端私密性相關的法律與管理問題。

第 8 章，稽核與制度

說明雲端內的稽核與制度之重要性，以及其他需要考量的各種標準和架構。

---

* Vaquero、Luis M.、Luis Rodero-Merino、Juan Caceres 等人。「A Break in the Clouds: Towards a Cloud Definition.」ACM SIGCOMM Computer Communication Review archive、第 39 冊，第 1 期（2009 年 1 月）。

第 9 章，雲端服務供應者範例

列出一些雲端服務供應者（CSP）為例，包括主要的 CSP（就規模與影響力而言），以及他們提供的服務為何。

第 10 章，安全即雲端服務

探討雲端運算安全性的另一種不同面向：將安全性作為透過雲端提供的服務。這種安全即雲端服務（security-as-a-[cloud] service，SaaS）也是正在開拓的領域，我們會在本章研究一些此類雲端安全服務。

第 11 章，雲端運算對於企業 IT 角色的衝擊

在雲端運算存在的今天，探討雲端運算對於企業 IT 部門的衝擊。雖然有些人認為雲端運算為 IT 部門補足了某些重要層面，但 IT 部門本身卻可能認為雲端運算取代了 IT 部門的許多責任。

第 12 章，結論與雲端的未來

總結本書所談的概念，並對雲端的未來提出一些看法。

本書也有字彙表，以及談論相關稽核格式（SAS 70 Type II 與 SysTrust）的三節附錄，並介紹一種稽核控制與雲端運算之間關係的模型。

本書編排慣例

本書所用的字體慣例如下：

楷體字或斜體字（*Italic*）

用來表示新名詞、網址與電子郵件。

定寬字（`Constant width`）

用來表示程式語言和指令程式元素。

附註

此圖示表示秘訣、建議或一般附註。

使用範例程式

本書的用意是協助你做好工作。通常而言，你可以在自己的程式與說明文件中使用本書的程式碼。你不需要為此向我們尋求允許，除非你要重製大部分的程式碼。例如，寫一個程式，其中用到來自本書的幾段程式碼，不需要經過允許。銷售或流通一張光碟，裡

面塞滿了 O'Reilly 書籍的範例程式碼，這就需要先徵求同意。回答問題時提及本書，並引用範例程式碼，不需經過同意。若從本書中取用大量範例程式碼，放在你自己的產品文件中，就必須先徵求同意。

雖無必要，但若能註明程式碼出處，我們會更感謝。註明出處時，通常要包括書名、作者、出版商以及 ISBN。例如「*Cloud Security and Privacy* by Tim Mather, Subra Kumaraswamy, and Shahed Latif. Copyright 2009 Tim Mather, Subra Kumaraswamy, and Shahed Latif, 978-0-596-80276-9.」

若你認為你的範例程式碼用途已經超出上述的允許範圍，請務必與我們聯繫：*permissions@oreilly.com*。

致謝

我們要感謝許多任職雲端服務供應商的人，他們願意花時間與我們詳談雲端的安全性與私密性。即使許多素材在書中並未明述出處，但能瞭解供應商對此課題的觀點，實屬無價之寶。我們也找了一些雲端運算服務的客戶洽談，實際瞭解他們的考量與體驗。為了完成本書，我們認為務必得收錄市場上最新的解決方案與趨勢。為此，我們與許多公司會面以瞭解當前趨勢。我們所談過的組織包括微軟、國家標準技術局與昇陽電腦。我們要感謝下列曾協助我們的人士：John Dutra、John Howie、Peter Mell、Izak Mutlu 與 Rajen Sheth。

我們也由衷感謝幾位花費時間檢查草稿，確保內容正確無誤，並使其更容易閱讀的人。感謝 Dan Blum、Robert Fly、Tim Grance、Chris Hoff、Jim Reavis、Laura Robertson 與 Rodney Thayer。本書中若有任何謬誤或不足之處，都是我們自己的責任，但這幾位已經盡力協助我們使錯誤減至最少。

幾位 KPMG 的員工也大力協助，在此感謝。他們提供內容、協助製圖、整理字彙表、協調面談時間、處理許多其他的工作，使我們的作業輕鬆得多。感謝 Graham Hill、Vijay Jajoo、Mark Lundin、Bob Quicke、Ismail Rahman、Doron Rotman 以及 Nadeem Siddiqui。

最後，在矽谷有此一說：「吃你自己的狗食。」行銷人員通常把這句話解釋成「用你自己家的產品。」嗯，當我們寫這本書時，我們確實乖乖吃自己的狗食，也就是儘量隨時隨地使用雲端服務。我們用雲端的電子郵件、行事曆，用其他雲端網站管理文件與圖片，以及聯絡 O'Reilly 的編輯（感謝你，Mike Loukides！）、校稿人、志工與使我們能隨時使用最新素材的 Lasselle-Ramsay。

Tim Mather 感言

我要感謝 Diva、Penny、Tiramisu 與 Sam 的全力支援，讓我過去一年能投入這麼多時間寫作。感謝我家的貓，能夠支持與諒解我。

Subra Kumaraswamy 感言

我很幸運，能獲得家人的愛與支持，即使犧牲了過去一年來的週末假期。由衷感謝愛妻 Preethika 以及兩個孩子 Namrata 與 Nitin。我也要感謝我的上司 Leslie Lambert（昇陽電腦的 CISO）能支持這項工作。此外我還要感謝朋友與同事們能協助校稿、廣為宣傳。

Shahed Latif 感言

我要感謝家人的支持與愛，即使我為了本書犧牲了許多週末、假日，加上許多漫漫長夜。我要特別感謝老婆 Moni、兒子 Ayaz，謝謝你們的支持與諒解。

目錄

第一章

簡介

「注意間隙」

如果你搭過倫敦的地鐵，你一定對這句話很熟：「注意間隙。」這是告訴你要小心月台和地下列車之間的間隙。地鐵月台與列車門之間，應當要前後對正左右標齊，但通常並非如此。有些地方，兩者之間的間隙大得誇張。所以，你得留意腳步。

我們可以用注意間隙的概念，當成雲端運算與其安全性的警告標語。理想而言，雲端運算與安全性這兩個概念，應當可以緊密接軌，但通常也並非如此。在這個高科技產業中，大家經常歌頌「雲端好，雲端妙」，同時卻又抨擊「雲端安全性不佳」。這到底代表什麼？雲端運算的安全性究竟有何問題？

本書的用意，在於透過系統化調查雲端由何構成、所提供的安全性為何，以回答上述問題。本書也會探討雲端運算對雲端服務供應商（CSP）與客戶的私密性、稽核與權責有何影響。雲端運算的安全性不佳嗎？

答案取決於你的雲端運算用途，以及你的期望。如果要將大型組織、大量資源整合成複雜的資訊安全專案，你就得克服許多安全性、私密性與權責上的難題，如本書往後所述。然而若只是中小企業（SMB），雲端運算的安全性與當今你預算所及的資訊安全而言，算是很吸引人的。

雲端運算的變革

雲端運算到底是什麼、不是什麼？為瞭解此問題，務必先認識這個運算模型的演變歷程。Alvin Toffler 在他的名著「第三波」（*The Third Wave*，Bantam，1980）中所述，文明的進展是分成三波（第一波是農業社會，第二波是工業時代，第三波是資訊時代）。

在每一波當中，都有幾個重要的浪潮。當前我們正處於工業時代之後的資訊時代，又是許多人所感受到的雲端運算時期開端。

在 Nicholas Carr 的著作「大轉變」（*The Big Switch*，W.W. Norton & Co.，2008）之中，他談到資訊時代的變革，與工業時代的一項重要變化多有相似。Carr 特別指出，資訊時代中的雲端運算興起，就像工業時代中的電力。企業組織以往必須自行提供動力（水車、風車）。但有了電，企業組織不再需要自行產生動力；他們只要接上電力網就行。Carr 認為雲端運算也會在資訊時代造成相同的改變。現今企業組織必須自行提供運算資源（動力）。至於未來，可能企業組織僅需將線路接上雲端（運算網），就能取得所需的運算資源。如他所述，「最後，外部應用程式所省下的花費實在太誘人，就連規模最大的企業也難以抗拒。運算網獲得勝利。」事實上，他著作中的第二篇就是談論「雲端生活」，以及雲端帶來的好處。（Carr 也深入探討了對這個大轉變所察覺到的負面社會影響，尤其是此轉變為社會帶來的黑暗面。）

Carr 並非唯一談論雲端運算益處的人，但他可能是至今最能清楚說明這些益處的一位。雖然他主要談論雲端運算在經濟上的益處，他並未提及與「大轉變」相關的資訊安全問題。我們非但要談，而且這就是本書的用意：詳述雲端運算「大轉變」相關的安全性與私密性問題。

如前所述，每一波之中都有多個浪潮，資訊時代之中已有幾個浪潮，如圖 1-1。我們從大型電腦開始，經歷小型電腦、個人電腦等等，如今正進入雲端運算。