IBM

IBM 觀點：
安全與雲端運算

雲端運算經過近兩三年的熱烈討論後，相關的雲端運算架構與應用已經逐漸成形，也出現許多實際導入雲端運算的商業模式。IDC 預測，臺灣企業2011年投入雲端服務的 IT 預算總值將達新台幣24億元，雲端運算服務將成為未來資訊應用的主要發展趨勢。

雲端運算擁有彈性、敏捷、降低成本、易於備援等好處，但安全性卻是一大隱憂。根據 IBM Market Insights, Cloud Computing Research 調查顯示，近7成受訪者對雲服務最大的疑慮是資料安全與隱私。

IBM

IBM 榮獲 SC Magazine 頒發「2010年最佳安全公司 (Best Security Company)」獎項，獲獎原因就在 IBM 在風險管理的優異表現，以及內容豐富又完整的資訊安全系列解決方案，可全面因應法規遵循、應用程式、資料、身分與存取管理、網路、威脅預防、系統安全、電子郵件、加密、虛擬化與雲端安全的需求，在資訊安全專精的深度或廣度都是產業之最。

SC MAGAZINE AWARDS 2010 WINNER Honored in the U.S.

雲端運算是彈性且符合成本效益的可靠平台，以「隨需應變」的方式提供所有程序、應用程式和服務。企業組織可善用雲端運算，來提高服務供應的效率、精簡 IT 管理，並且根據動態的商業要求有效調整 IT 服務，為核心商業功能提供可靠的支援，優化開發創新服務的能力。

目前業界使用的雲端運算可分為公有和私有雲端模型；公有模型是任何有網際網路存取權的人都可使用，私有雲端則為單一組織所有。許多企業組織同時採用這兩種雲端運算，將其納入混合式雲端，以達到特定商業和技術要求，不僅提供最佳安全和隱私功能，還可將固定 IT 成本投資降至最低。

儘管雲端運算的好處很明確，但也需要針對雲端實作開發適當的安全機制。接下來將探討雲端運算的重要安全問題，然後針對安全雲端架構與環境提供 IBM 觀點。

因應雲端安全性：一項艱巨挑戰

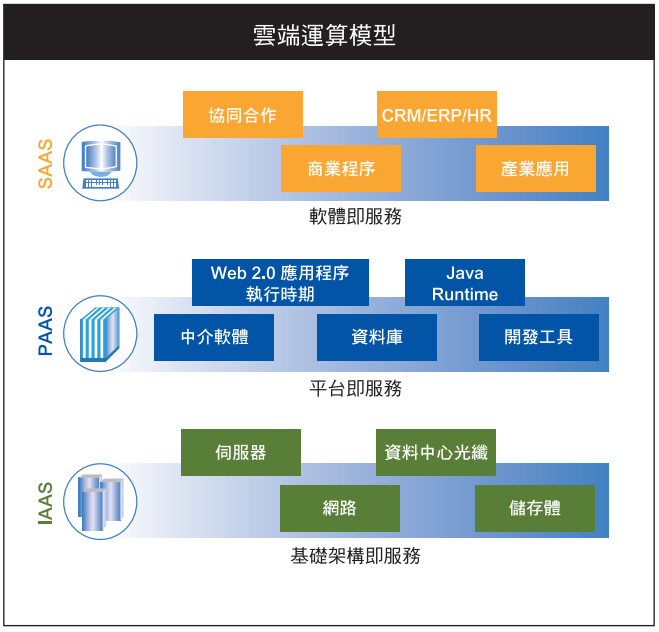
委外作業的「外部化」，導致企業很難維持資料完整性及隱私權、支援資料與服務的可用性，以及證明法規遵循狀況。另外，雲端內部很難找到資料的實際儲存位置，曾經可見的安全程序如今都已隱藏在抽象層後面；這種無法查看的缺點，可能會導致許多安全和法規遵循問題。因此，有些企業組織選擇私有或混合模型，而不採用公有雲端。

雲端運算廣泛共用基礎架構，其安全性和一般 IT 環境安全迥異，需要高度標準化和程序自動化，以便降低操作者發生錯誤或疏忽的風險，進而提高安全性；雲端運算模型仍須重視隔離、身分識別和法規遵循。

評估雲端運算的不同模型

不同的雲端運算模型，使用者接觸的方式也不同，因而影響直接控管運算基礎架構的能力及其安全管理責任歸屬。

軟體即服務 (SaaS) 模式中，多數安全管理責任在於雲端供應商； SaaS 提供多種 Web 入口網站的存取控制方式，如管理使用者身分、應用程式層次配置，以及限制存取特定 IP 位址範圍或地區。平台即服務 (PaaS) 模式中，用戶端承擔較多中介軟體、資料庫軟體和應用程式執行時期的配置和安全性管理責任。在基礎架構即服務 (IaaS) 模式中，用戶端更進一步掌握更多安全控管權利和責任，例如，可存取支援虛擬影像、網路和儲存體的作業系統。



許多企業組織都深受雲端運算的彈性和成本效益所吸引，但也十分關切安全問題。短期內，大部分企業會善用外部雲端供應服務，處理低風險的工作；一體適用的安全措施雖然保障較少，但成本也較低。至於涉及高度受管理或專屬資訊的中高風險工作，企業會選擇私有及混合雲端，以取得必要的控制權和保障。

IBM 安全架構

IBM 安全架構旨在說明需受保護的商業資源安全性，並從企業觀點分析不同的資源領域。

安全控管、風險管理和法規遵循

企業需要雲端安全狀態的監視功能，供應商則因必須支援第三方的審核，譬如協助客戶在疑似違規事件發生時，支援電子探索及鑑識調查；此時，資訊透明度對法規遵循顯得尤其重要。

人員及身分

雲端環境通常支援大量且異質的使用者社群，企業必須確定公司及供應鏈的授權使用者，可以隨時存取所需資料和工具，同時攔截未經授權的存取，特許使用者也必須受到實體監視和背景調查；身分聯合及快速啟用功能、標準型單一登入功能，亦不可或缺。

資料與資訊

在雲端儲存體基礎架構上，所有機密性或受管制資料，都需要適當區隔，並透過資料加密金鑰，保護資料隱私權和遵守法規。而加密行動式媒體，以及這些加密金鑰的共用問題，也不應被忽視。雲端運算的資料配置，可能會因為企業所在位置、資料種類及商業性質，受到嚴重限制，或造成智財權的嚴重威脅。

應用程式與程序

影像安全，是雲端應用程式安全要求的重點。雲端應用程式適用一般應用程式的安全要求，管理這些應用程式的影像檔亦是；雲端供應商必須遵守並支援安全的開發流程，協助雲端使用者的影像檔保存、授權及使用控制。影像檔若需暫停使用或銷毀，應格外謹慎，以免機密資料外洩。

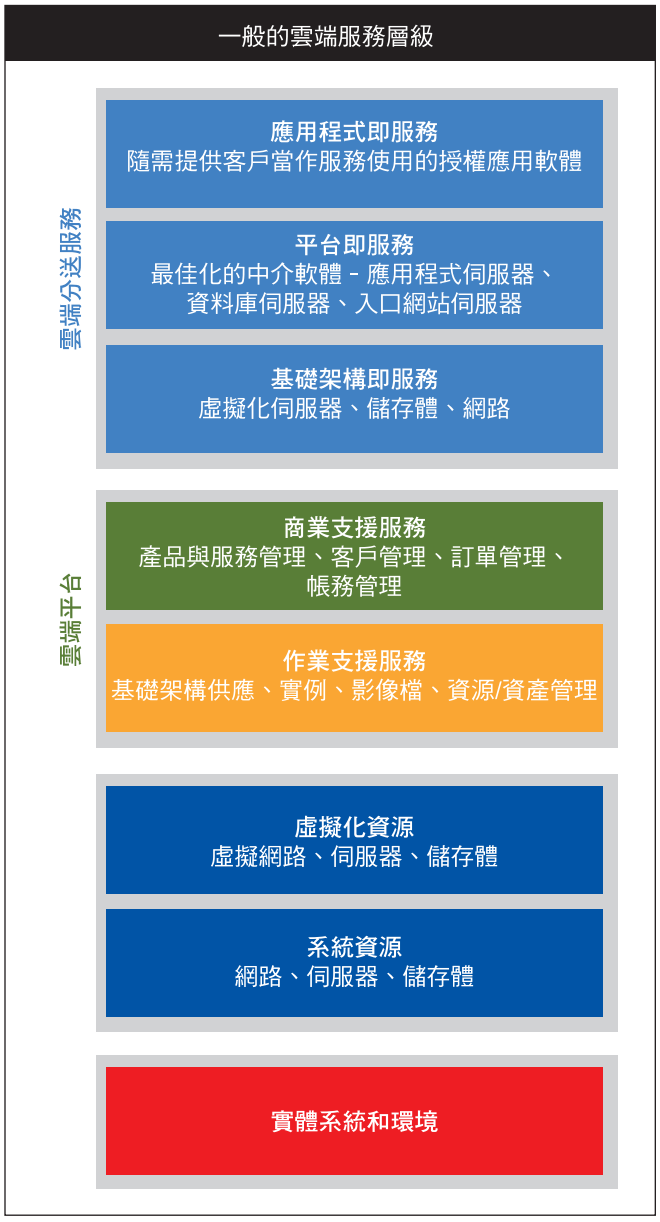
網路、伺服器及端點

資料越難控管，客戶就越期待雲端環境能內建類似入侵偵測與防禦系統等功能。雲端基礎架構必須確保實體安全，供應商亦需清楚說明，實際存取客戶工作量及支援客戶資料的伺服器，如何管理。

瞭解 IBM 的雲端安全性觀點

資訊安全是一個不斷改變的目標，必須定期檢查環境，防止常見的威脅及漏洞。此外，企業要移轉至雲端的業務工作量，有其專屬特性，安全需求也不一樣；「一體適用」的安全方案並不存在。對於雲端環境與企業後端系統的整合，多數企業客戶會先採用混合或私有雲端，透過各類聯合通訊協定，將現有安全管理基礎架構擴充到雲端。

因應不同的工作量及工作類型，企業在第三方安全審核或驗證、加密、以及可用性方面，安全需求的等級也不同。IBM 認為，企業級雲端服務供應商必須支援廣泛的安全和服務層次方案，安全基礎架構，則必須能輕鬆整合現有作業。服務供應商也必須依客戶需求，隨時整合及擴充其雲端安全功能。



雲端運算的基本架構模型

雲端運算的基本架構模型是由一組分層服務組成。實體系統層說明了一般資料中心的需求，以強制執行存取控制措施和監視設備。系統資源層負責控管網路、伺服器和儲存體基礎架構。虛擬化資源層可建立強大的隔離機制，作為虛擬化安全的核心資產：透過 Hypervisor 及資料分離，區隔各程序。

作業支援服務 (OSS) 層和商業支援服務 (BSS) 層，可定義雲端管理平台。頂層是基礎架構即服務、平台即服務和應用程式即服務的不同雲端分送服務。

此架構的各個層級都有安全需求，而且必須維持各層之間的一致性。比方說，如果最頂層的安全原則規定不能將客戶資訊傳到國外，那麼在實體資源的較底層，就必須將儲存這些資料的磁碟空間配置在國內。

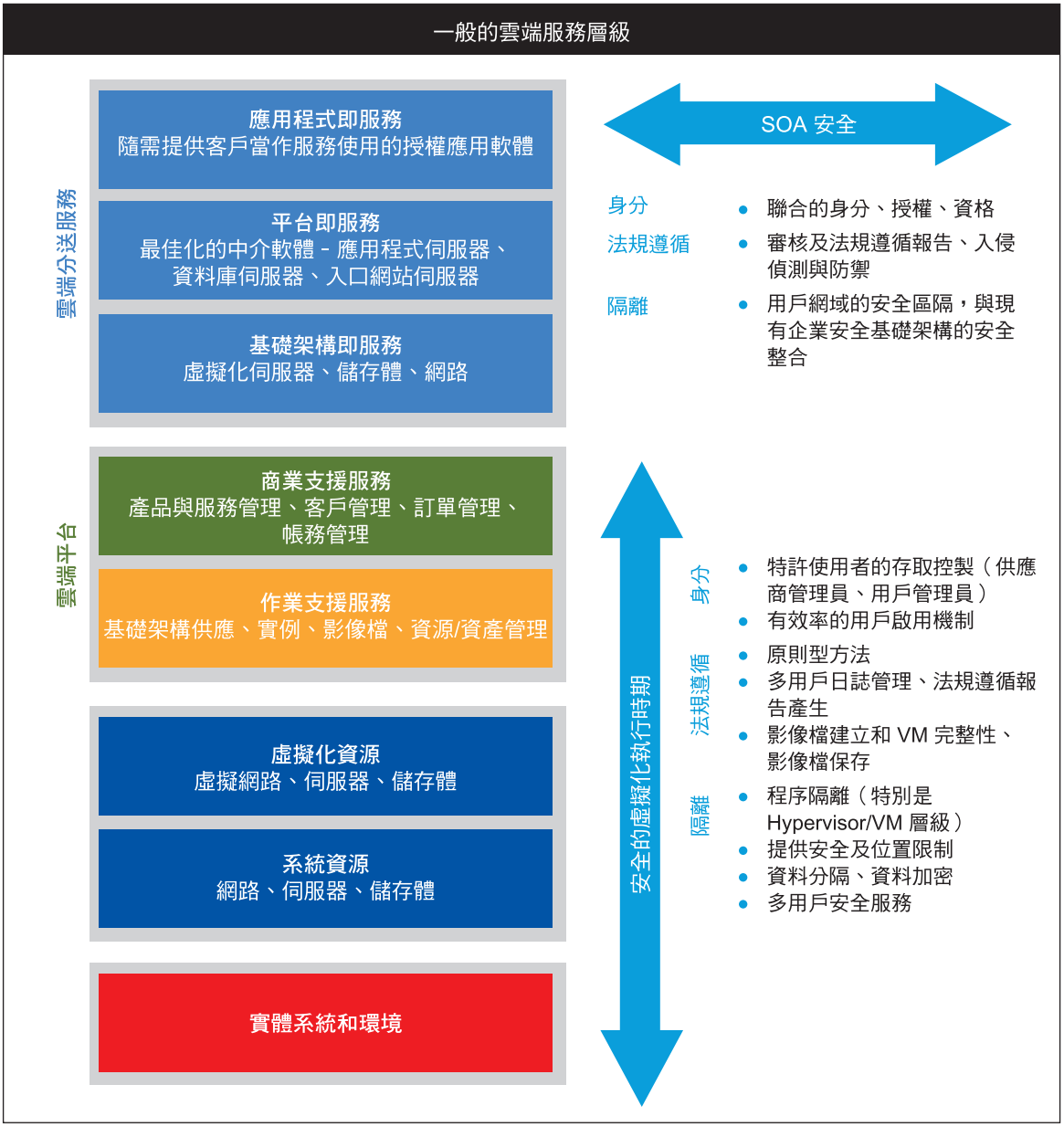
雲端安全和 SOA

企業內的不同雲端可互相傳送不同服務，Web 服務 (WS) 通訊協定堆疊構成 SOA 安全及雲端安全的基礎。雲端運算可支援大量租戶、服務及標準，比多數企業的 SOA 環境更勝一籌。這種十分彈性靈活的支援，信任關係也較為複雜，尤其雲端 SOA 雖支援大量開放的使用者群，但不隨意接受雲端供應商和用戶之間預先建立的關係。

為確保雲端服務的機密及合規需求，授權和存取控制原則必須一致。供應商也應遵守最佳實作方法，提供客戶最大透明度，檢視雲端服務安全性和法規遵循狀況。在 Secure Virtualized Runtime 中，安全服務也逐漸透過 SOA 服務具體化，以提供身分、審核、金鑰管理、原則及其他服務。

簡化安全控制與防禦的契機

雲端運算雖然帶來更多安全風險和新的威脅媒介，也是改善安全性的大好機會。標準化、自動化和加強的基礎架構透明度等雲端特性，皆可大幅提升安全層次。例如，使用定義的雲端介面組合及集中管理的身分與存取控制原則，可降低使用者存取非相關資源的風險。在隔離網域中執行運算服務、資料的預設加密，透過虛擬儲存體進行的資料控制，都可以改善可靠性，並減少資料流失。



雲端安全建議

IBM 的全球研究員、開發人員及安全專家已取得3,000 多個安全和風險管理專利。依據IBM研究團隊及客戶經驗，雲端安全措施分為以下8大類，共計25項要點：

（一）建置安全計畫

1. 安全計畫應衡量組織文化對於安全的需求，並依重要性決定優先部署順序。除了定義雲端的潛在威脅並加以控制，也應參考產業規定或最佳實例，制定可監控及衡量的矩陣，同時發展出究責結構以及回應步驟。企業須確保雲端建置團隊了解並支援相關行動計畫，同時進行內部教育訓練，讓所有管理者了解安全政策。企業應建置能掌控安全狀態及異常事件的系統、稽核計畫、執行架構、以及訊息通知計畫。

（二）建置安全的雲端基礎架構

2. 為維護防火牆的組態設定，變更管理程序應有正式簽核及接受組態調整。防火牆應設置在與外部網路的每一界接處，以及雲端每個安全區域間。網路架構、資訊流及防火牆的設置，要考慮到虛擬環境及軟體防火牆；企業營運持續所需的服務及通訊埠，應整理成文件並妥善維護。防火牆的通訊埠應預設為關閉；針對防火牆通訊協定的例外狀態及異常的定義，應進行驗證或風險評估。

   防火牆應拒絕來自未被信任的來源或應用程式存取，並予以記錄。對於直接外部連線、存有機密資料或組態設定資料的系統，防火牆應限制其存取。在外部設備或移動裝置中，個人防火牆的介面及雲端環境，應由雲端供應商應支援。防火牆應進行IP遮罩，避免內部系統架構被輕易探查，並確保所有機密資料都存放在防火牆之後。

其他要點包括：

3. 不要使用供應商預設的密碼或安全參數
4. 保護管理者的存取控制及安全連線
5. 確保修補程式的管理
6. 實體環境的安全
7. 適當保護遠端與企業基礎架構之間的連線溝通

（三）機密資料的保護

8. 個人資料的保護：參酌產業特殊需求，從個資的蒐集取得、處理、傳輸、儲存到銷毀，須制定一套規則，並制定個資外洩通知策略以及個資盤點及分類計畫，維持個資數量的最小化。
9. 非必要個人資料的安全銷毀：個資在系統顯示時應適當遮罩，確認個資不會被記錄在日誌檔或其他系統檔案中，所有個資調閱動作亦應予以記錄。
10. 機密企業資料的保護：比照個資的方式，在資料搬上雲端前應進行資料衝擊評估，衡量企業風險忍受度。
11. 智慧財產的保護：應進行風險評估，確認公有雲供應商的 SLA 協議內容涵蓋智慧財產。資料搬上雲端前，企業應使用加密等技術，確保系統不易被逆向工程破解。
12. 加密金鑰的保護：制定並執行金鑰儲存管理計畫，包括安全的金鑰配置及管理方法，至少每年一次定期回收金鑰，將過期失效的金鑰予以銷毀。金鑰若疑似被複製外洩，應有立即中止或替換機制與通知程序，避免金鑰在非授權下被替換。金鑰應具有雙重共有控制機制，儲存位置盡量減少，所有存取都要留下記錄。

其他要點包括：

13. 利用 SSL/TLS 和 IPSEC 安全通訊協定，確保資料傳遞溝通的安全。
14. 導入防制資料外洩 (DLP) 機制
15. 確保應用程式所處理的資訊都被安全保護

（四）強固的存取及身分管理

16. 最低權限的架構：應確保使用者的存取權限是適當的，存取機制受到安全保護。包括要定期檢查使用者存取權限列表，使用個人憑證搭配遠端 VPN 存取管理者功能，將密碼的傳送及儲存加密，所有系統都應有認證及密碼管理功能。
17. 聯邦式的身分管理：當要界接各種雲端環境時，聯邦式的身分管理十分重要。許多企業部署雲端會從建置私有雲或混合雲開始，與原有 IT 後端系統的整合成為重要課題；部署成功與否，端視企業現有的安全管理架構是否能延伸到雲端。

（五）建立應用程式與環境的自動佈建

18. 應用程式自動佈建計畫：虛擬影像檔的自動佈建應符合權限控管及授權，具安全及銷毀機制。虛擬資源應依照政策組合搭配，透過自動化安全組態管理，確保設定一致；在安全的虛擬化環境中，仍須以 SOA 方式提供安全機制。

（六）建立 IT 治理及稽核管理計畫

19. 隱私管理計畫：個人及企業機密資料的蒐集、處理、利用、刪除，都需建立政策文件以及監控稽核程序；企業內部應進行教育訓練，並訂定資料外洩事件通知程序，讓稽核人員及管理階層瞭解雲端環境的個資安全威脅。
20. 稽核管理計畫：檢視雲端系統必須符合哪些法規，建立相關規範文件並定期檢視。
21. 資料安全的合規：資料的處理、儲存，應遵照法規及跨境保護要求辦理，並整理成文件，政府單位尤其需要正式的驗證或證書。

（七）建立弱點及入侵管理計畫

22. 定期更新防毒、入侵偵測 / 防禦系統。

（八）測試與驗證

23. 導入變革管理的程序：雲端系統必須遵照組態變更管理程序，包括變更請求須留下記錄、衝擊評估說明、上線前測試結果並簽核、回復到前一階段的程序。
24. 導入資料加密及存取計畫：測試資料庫及其他儲存媒介透過適當加密技術受到保護。
25. 發展安全的應用程式開發及測試計畫：所有修補程式在上線部署前，需要經過驗證；測試及開發環境需予以區隔，並劃分不同人員負責測試、開發及管理的工作。正式系統中所含機密資料或個資不應流入測試環境；測試環境正式上線前，應移除所有測試資料或管理資訊，並進行原始碼檢測。所有網頁應用程式，應遵照 IBM 或 OWASP 等安全程式碼準則，定期進行檢測。

總結

許多人認為雲端運算資訊安全風險更高，但若以另一角度思考，由於雲端運算的標準化、自動化，以及對 IT 基礎架構的透明掌握度增加等特性，這也是個重新提升安全水準的契機。

IBM 可提供無與倫比的功能，以便您致力於企業創新，同時保護所有風險網域的作業程序。其包羅萬象的解決方案和服務可讓企業降低公司內部的安全複雜性，並實施全方位的安全管理策略。在 IBM 的協助下，企業可開發各種各樣可調式標準型解決方案，以支援目前和未來的安全需求。

進一步資訊

如需雲端運算的詳細安全性資訊，請聯絡您的 IBM 業務代表或 IBM 事業夥伴，或者造訪 ibm.com。您也可以瀏覽下列網站，取得雲端安全性的其他資訊：

IBM 軟體雲端：www.ibm.com/software/tw/cloud

IBM 企業資訊安全：
http://www.ibm.com/software/tw/info/itsolutions/security/

IBM 智慧軟體：http://www.ibm.com/software/tw/

台灣國際商業機器股份有限公司
台北市松仁路7號3樓
市場行銷處：0800-016-888按1
技術諮詢熱線：0800-000-700

台灣印製
2011 年 03 月