雲端運算
白皮書
2009 年 11月

IBM 觀點：
安全與雲端運算

目錄

前言

雲端運算是彈性且符合成本效益的可靠平台，可透過網際網路提供商業或消費性 IT 服務。無論使用者位置或裝置爲何，皆可快速部署及輕鬆擴充雲端資源，以「隨需應變」的方式提供所有程序、應用程式和服務。

因此，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。雲端運算在許多方面都可以針對下列兩個領域提供最佳效能：爲核心商業功能提供可靠的支援，以及開發創新服務的能力。

附加好處是，雲端運算可在不增加複雜性的情況下加強使用者體驗。使用者不必瞭解任何基礎技術或實作。

目前業界使用的雲端運算可分爲公用和專用雲端模型。公用模型是任何有網際網路存取權的人都可使用，其中包括軟體即服務 (SaaS) 雲端（如 IBM LotusLive™）、平台即服務 (PaaS) 雲端（如 IBM Computing on Demand™），以及安全與資料保護即服務 (SDPaaS) 雲端（如 IBM Vulnerability Management Service）。

專用雲端則爲單一組織所有。這些模型可提供許多公用雲端的好處，讓企業組織擁有更大的彈性和控制功能。此外，專用雲端在資料流量尖峰期間的傳輸延遲率比公用雲端低。因此，許多企業組織都同時採用這兩種雲端運算，將其納入混合式雲端。這些混合雲端可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

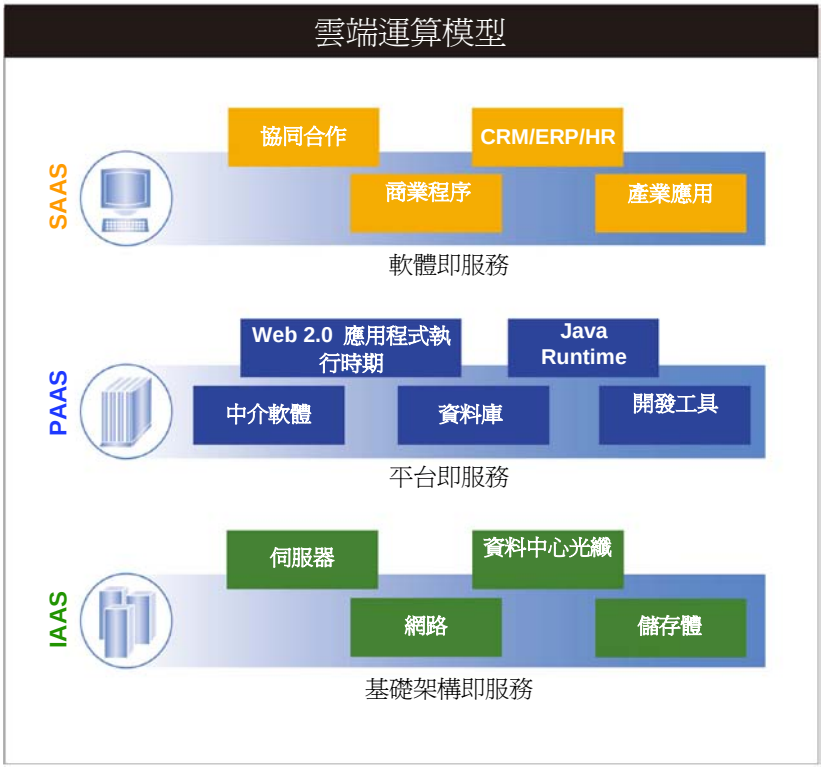
由於重要服務通常是外包給其他業者，所以除了開發安全 IT 系統的一般難題之外，雲端運算還面臨多一層風險。委外作業的「外部化」導致企業很難維持資料完整性及隱私權、支援資料與服務的可用性，以及證明法規遵循狀況。

實際上，雲端運算已導致客戶組織必須將多許資料和作業的控制權轉交給雲端供應商，就像委外部分 IT 作業一樣。即使是套用修正程式和配置防火牆等基本工作，也可能變成雲端服務供應商的責任，而非一般使用者。因此，客戶必須與供應商建立起信任關係，並瞭解這些供應商代爲執行、部署和管理安全性的潛在風險。然而，儘管工作量已移至雲端，客戶還是法規遵循和保護重要資料的最終負責人，所以這種雲端服務供應商與客戶之間的「信任但需確認」的關係就十分重要。鑑於委外服務的相關風險，有些企業組織選擇專用或混合模型，而不採用公用雲端。

其他雲端運算層面也需要重新審慎評估安全性和風險。在雲端內部，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。

此外，雲端運算會廣泛共用基礎架構，所以其安全性和一般 IT 環境安全迥異。來自不同企業及信任層級的使用者會與同一組運算資源互動。同時，在現今動態的 IT 環境中，工作量平衡、不斷變更的服務水準協定 (SLA) 及其他層面，都使不當配置、資料外洩和惡意行爲的發生機率大爲增加。

基礎架構共用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。不過，廣泛共用的基礎架構本身存在一定風險，雲端運算模型還是必須重視隔離、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，使用者接觸其基礎架構的方式也不一樣。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。

如果是 SaaS 模型，多數安全管理責任在於雲端供應商。SaaS 可提供多種 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。

平台即服務的雲端模式則允許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。如果是基礎架構即服務 (IaaS) 模型，用戶端可掌握更多安全控管權利和責任。在此模型中，可存取支援虛擬映像、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。產業分析師所提出的最新雲端技術使用研究和媒體報導都證明確實有這方面的顧慮，其中提到外部管理的共用環境缺乏透明度與控制權、機密性資訊保護及受管制資訊的儲存問題。

如果要針對重要 IT 服務大量使用外部共用、完全開放的雲端運算平台，恐怕還要好幾年才能實現。

短期內，大部分數企業會採取善用外部雲端供應服務的方法。這些雲端主要用來處理低風險的工作，可接受較少保障的一體適用安全措施，而其價格則是主要差異化因素。至於涉及高度受管理或專屬資訊的中高風險工作，企業會選擇專用及混合雲端，以取得必要的控制權和保障。直到外部雲端可提供更嚴謹、更彈性的安全功能後，才會將這些工作委外。

檢視 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。

下節根據 IBM 安全架構及與 IBM 客戶廣泛討論的結果，列出了現今企業級雲端運算的主要安全要求。（如需相關資訊，請參閱 *IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security*，IBM RedGuide REDP-4528-00，2009 年 7 月。）

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。其中包括廣泛的變更、映像和事件管理監視功能，還有租戶、特定租戶記錄及審核資料的事件報告。

資訊透明度對法規遵循尤其重要。沙賓法案、健康保險便利及責任法案 (HIPAA)、歐洲隱私權法及其他法規都需要詳細的審核功能。因此，對用戶而言，公用雲端就像「黑盒子」，潛在雲端用戶可能無法證明法規遵循狀況。（專用或混合雲端在經過配置之後，則可滿足這些要求。）

此外，供應商有時必須支援第三方的審核，疑似有違規事件發生時，客戶可能會被要求支援電子探索及鑑識調查。此時，適當的雲端透明度就更加重要了。

一般上，企業會根據他們的策略性委外和一般受管理服務經驗，要求彈性的 SLA 以因應特定狀況。

人員及身分

企業必須確定公司及供應鏈的授權使用者可隨時存取所需資料和工具，同時攔截未經授權存取。雲端環境通常支援大量各種各樣的使用者社群，所以這類控制功能愈加重要。此外，雲端可建立一層新的特許使用者等級：雲端供應商的管理者。特許使用者監視（包括記錄活動）已成爲一項重要需求。此監視功能應該包括實體監視和背景調查。

同時，必須有身分聯合及快速啓用功能，以協調企業後端或第三方系統的驗證及授權作業。若要簡化內部應用程式及雲端的使用者登入，必須有標準型單一登入功能，以便使用者輕鬆快速地使用雲端服務。

資料與資訊

大部分企業都提到，資料保護是最重要的安全問題。典型的顧慮包括資料的儲存和存取方式、法規遵循及審核要求，以及資料外洩成本、通知要求和品牌價值損失等商業問題。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，包括保存的資料。

無論是傳送至雲端或儲存在服務供應商資料中心的資料加密金鑰，都必須加密及管理，才能保護資料隱私權和遵守法規。而加密行動式媒體，及在雲端服務供應商和消費者之間安全共用這些加密金鑰，則是經常被忽略的重要需求。由於很多時候無法透過網路以快速、低成本的方式移動大量資料，許多企業還是必須將行動式媒體（如保存磁帶）交給雲端供應商。最重要的是，資料必須加密，而且只有雲端供應商和客戶可存取加密金鑰。

雲端運算可能會因爲企業的所在位置、處理的資料種類及商業性質，而嚴重限制資料配置。例如，有幾個歐盟成員國就明確表示禁止將國人的非公開個人資訊傳到歐盟以外的地區。

數個美國州政府亦禁止將員工的非公開個人資訊送到海外。

此外，雲端部署不僅可能帶來加密資訊相關的出口法律違規問題，也可能導致智財權受到嚴重威脅。公司的法律顧問必須在部署雲端之前，先全盤審查這些要求，確定公司可以充分控管供應商基礎架構中的資訊地理位置。

對於已明確指出使用者和資料有不同風險等級的領域（如公共和金融服務），企業必須進行整體的雲端資料分類。資料分類可控管誰可以存取、資料的加密和保存方式，以及如何使用技術防止資料流失。

應用程式與程序

一般上，客戶會考量映像安全方面的雲端應用程式安全要求。所有一般應用程式安全要求仍適用於雲端應用程式，而且沿用於管理這些應用程式的映像檔。雲端供應商必須遵守及支援安全的開發流程。此外，雲端使用者需要映像檔保存、授權及使用控制方面的支援。暫停使用及銷毀映像檔時也必須格外謹審，以免映像檔中的機密資料外洩。

定義、驗證和維護特定客戶安全原則的相關映像檔安全狀況是十分重要的要求，尤其是嚴格管制的產業。企業必須確定發佈到雲端的 Web 服務是安全、符合法規及商業原則。善用安全開發最佳實務是一項關鍵需求。

網路、伺服器及端點

在共用的雲端環境中，客戶想要確定所有用戶網域都經過適當隔離，而且不會將某用戶網域的資料或交易外洩到其他網域。爲了達到此目的，客戶需要配置受信虛擬網域或原則型安全區的功能。

資料越難受控，客戶就越希望雲端環境可內建類似入侵偵測與防禦系統的功能。客戶的顧慮不僅是擔心受信虛擬網域遭入侵，還有資料外洩及「對外輸出」，也就是不當使用客戶的網域在第三方裝載攻擊。將資料移至外部服務供應商，則會加深發生內部及網路阻斷服務 (DoS) 或分散式阻斷服務 (DDoS) 攻擊的隱憂。

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。

在共用環境中，各方都必須針對檢查資料的責任達成共識，並定期執行審查。企業必須主控合約管理以進行風險評估，或不是直接執行的控制部署。

凡事由雲端供應商提供的映像檔目錄，客戶都要確保這些映像檔安全且受到適當保護，以免毀損或遭濫用。許多客戶希望這些映像檔受到加密認證及保護。

實體基礎架構

雲端基礎架構必須確保實體安全，包括伺服器、路由器、儲存裝置、電源供應及其他支援作業的元件。這些保障包括使用生物特徵存取控制法及閉路電視 (CCTV) 監視系統，充分控管和監視實體存取。供應商需要清楚說明如何管理實際存取儲存客戶工作量及支援客戶資料的伺服器。

瞭解 IBM 的雲端安全性觀點

IBM 根據在各垂直產業設計、導入和支援雲端運算解決方案的豐富經驗，提供了明智的雲端安全性觀點。

沒有「一體適用」的安全方案

在雲端技術領域中，並沒有所謂的一體適用安全模型。企業要移轉至雲端的業務工作量有其專屬特性，因此安全需求也不一樣。

對於雲端環境與企業後端系統的整合，各企業要求不盡相同。有些企業要開發全新的應用程式，準備打造獨立於現有作業之外的雲端環境。但多數企業客戶會先採用混合或專用雲端，這種方式的主要需求是整合企業系統。

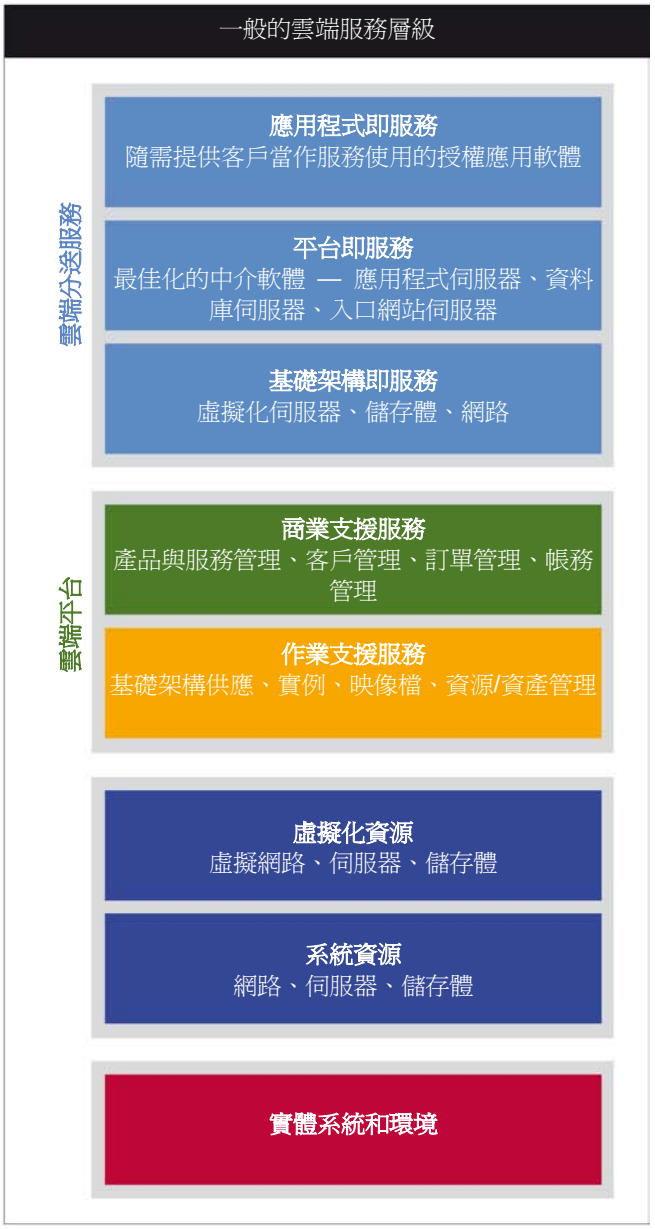
在此情況下，可輕鬆將現有安全管理基礎架構擴充到雲端，尤其是使用聯合通訊協定時，通常可順利完成部署。OpenID 及安全主張標記語言 (SAML) 等身分聯合通訊協定雖備受矚目，且對公用雲端十分重要，但企業必須支援各種不同的其他通訊協定。這些通訊協定的共同目標就是從企業後端系統，將資料快速移至專用或混合雲端。

不同的工作量需要不同的安全等級。其中一項首要需求就是第三方安全審核或驗證，有些政府甚至要求正式驗證和憑證。根據工作量類型而定，身分證明（確定登入服務的使用者真實身分）及鑑別機制的強度會有所不同。因此，目前已有新的身分驗證公用服務，可提供不同程度的服務品質。

各客戶的加密要求也迥然不同。有些客戶規定使用特定加密演算法，嚴格限制可以存取金鑰的使用者；有的客戶則只需要加密特定資料，並委託可靠的雲端服務供應商進行金鑰管理。

可用性要求更是林林總總，如供應商因應及進行失效回復的時間限制。執行安全和相符性檢查的時間間隔也不一樣。

IBM 認爲，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，以及可輕鬆整合現有作業的可延伸產業標準型安全基礎架構。此外，服務供應商必須視需要，隨時整合及擴充客戶的雲端安全功能。

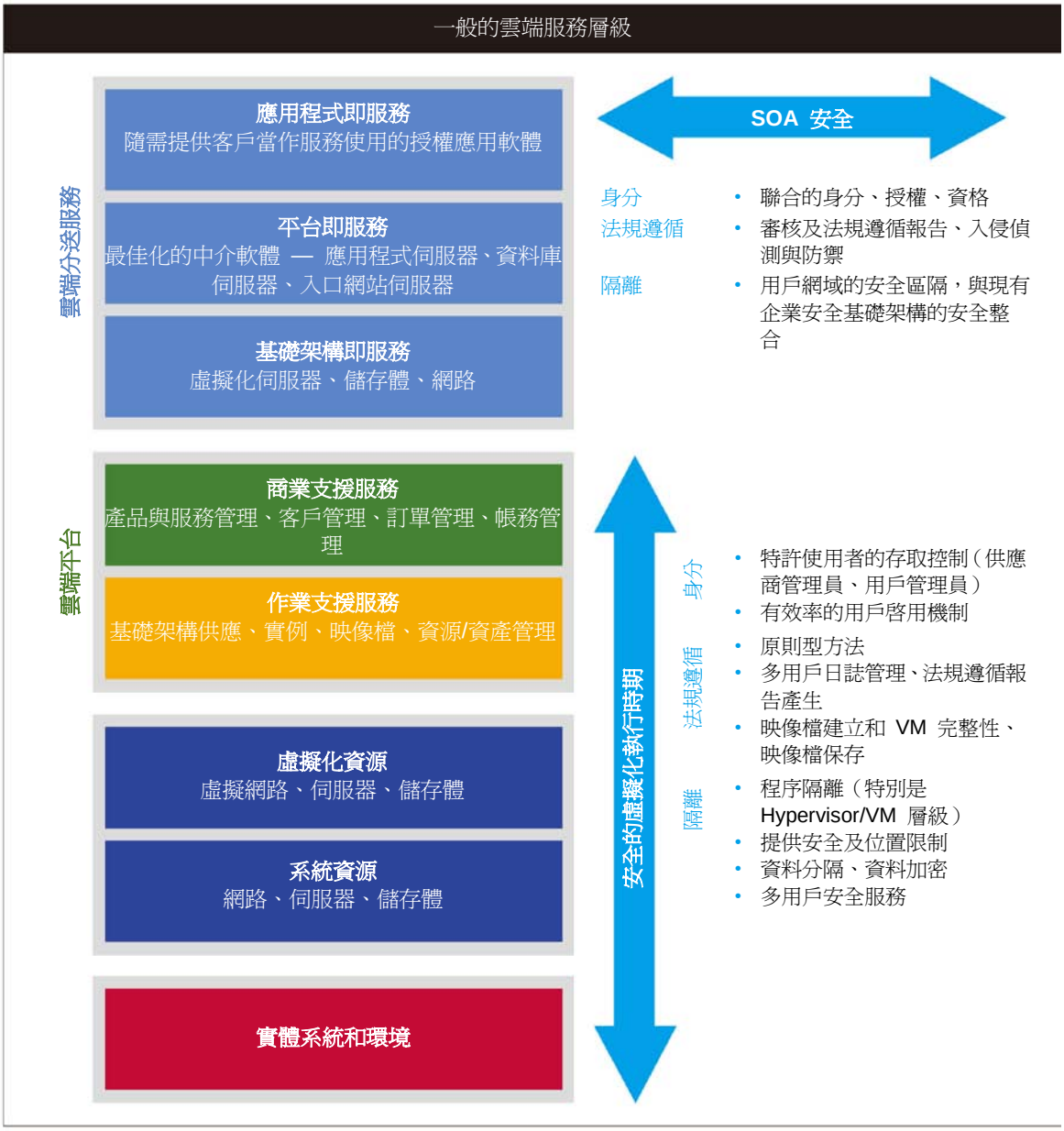

一般的雲端服務層級
雲端分送服務
應用程式即服務
隨需提供客戶當作服務使用的授權應用軟體
平台即服務
最佳化的中介軟體 — 應用程式伺服器、資料庫伺服器、入口網站伺服器
基礎架構即服務
虛擬化伺服器、儲存體、網路
雲端平台
商業支援服務
產品與服務管理、客戶管理、訂單管理、帳務管理
作業支援服務
基礎架構供應、實例、映像檔、資源/資產管理
虛擬化資源
虛擬網路、伺服器、儲存體
系統資源
網路、伺服器、儲存體
實體系統和環境

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，作爲虛擬化安全的核心資產：透過 Hypervisor 及資料分離，區隔各程序。

接下來是作業支援服務 (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。


一般的雲端服務層級
雲端分送服務
應用程式即服務
隨需提供客戶當作服務使用的授權應用軟體
平台即服務
最佳化的中介軟體 — 應用程式伺服器、資料庫伺服器、入口網站伺服器
基礎架構即服務
虛擬化伺服器、儲存體、網路
雲端平台
商業支援服務
產品與服務管理、客戶管理、訂單管理、帳務管理
作業支援服務
基礎架構供應、實例、映像檔、資源/資產管理
虛擬化資源
虛擬網路、伺服器、儲存體
系統資源
網路、伺服器、儲存體
實體系統和環境
SOA 安全
身分
法規遵循
隔離
• 聯合的身分、授權、資格
• 審核及法規遵循報告、入侵偵測與防禦
• 用戶網域的安全區隔，與現有企業安全基礎架構的安全整合
安全的虛擬化執行時期
身分
法規遵循
隔離
• 特許使用者的存取控制（供應商管理員、用戶管理員）
• 有效率的用戶啓用機制
• 原則型方法
• 多用戶日誌管理、法規遵循報告產生
• 映像檔建立和 VM 完整性、映像檔保存
• 程序隔離（特別是 Hypervisor/VM 層級）
• 提供安全及位置限制
• 資料分隔、資料加密
• 多用戶安全服務

雲端安全和 SOA

此雲端架構可建立非常簡單的雲端安全模型，其中包含兩個主要概念：位於新安全虛擬化執行時期層頂端的 SOA 安全層。

雲端分送服務 (Cloud Delivered Services) 層是複雜的分散式 SOA 環境。企業內的不同雲端可互相傳送不同服務。這些服務可能是在組成單一雲端應用程式的不同管理或安全網域中。SOA 安全模型可充分運用到雲端。Web 服務 (WS) 通訊協定堆疊構成 SOA 安全及雲端安全的基礎。IBM 軟體堆疊即可充分支援此安全模型。（如需這些產品和 SOA 安全模型的相關資訊，請參閱 IBM 紅皮書 SG24-7310-01，*Understanding SOA Security*）。像 IBM Tivoli® Federated Identity Manager 這種解決方案可提供廣泛的標準型支援，聯繫不同安全網域，以便使用者隨時存取雲端服務。利用混合雲端模型整合內部 IT 資源及第三方雲端服務時，或者是在一般客戶產品中納入多種第三方服務時，此功能尤其重要。

SOA 的其中一項優勢是可輕鬆整合不同供應商的服務。雲端運算比多數企業 SOA 環境更勝一籌，因爲雲端可支援大量租戶、服務及標準。這種支援是以十分彈性靈活的方式，在極複雜的信任關係下提供。特別是，雲端 SOA 有時可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。

許多雲端實作都著重在特定通訊協定（如用於身分聯合的 OpenID），而且偏好特定架構樣式，如代表性狀態傳輸 (REST)。IBM 認爲，企業級雲端運算不能限制使用者只使用特定通訊協定或樣式，應提供適度彈性和選擇。儘管 IBM 會適當支援 REST 型介面和通訊協定，SOA 安全仍需全方位的安全服務，如 SOA Security Reference Model 所述。

SOA 的基本概念是將安全具體化爲服務，以便其他服務使用。

透過標準準則驗證、登記和鑑別雲端服務使用者，只是確保相關使用者有適當資源存取權的方法之一。若要確保雲端服務的所有元件維持資料機密性並符合法規要求，就需要一致的授權和存取控制原則。例如，某醫療研究應用程式會從診所擷取資料，並從不同醫院取得計費服務，因此所有資料來源都必須移除病患姓名和其他個人識別資訊。集中管理的授權管理服務（如 IBM Tivoli Security Policy Manager）有助於確保定義及執行共同原則，以保護所有雲端服務中的病患隱私。

雲端供應商可支援雲端中及雲端之間的 SaaS 和 IaaS。供應商應遵守最佳實作方法，並提供客戶最大透明度，以檢視雲端服務安全性和法規遵循狀況。IBM Rational® AppScan® 產品組合可支援應用程式安全。IBM Tivoli Security Information and Event Manager 則可綜合檢視安全審核日誌及預先內建的報告，以證明法規遵循狀況及識別特許內部人員的潛在威脅。在第三方管理員可存取不同企業資料的公用雲端模型中，監視及因應特許 IT 管理員威脅的能力就更爲重要了。

底端的安全虛擬化執行時期層是一個虛擬化系統，此系統所執行的程式會提供資料儲存庫的資料存取權。這個執行時期是在虛擬機器上執行，而不是在個別應用程式上的一般執行時期系統。其提供的安全服務有防毒、內部檢查及虛擬映像的相關具體化安全服務。

雖然 Secure Virtualized Runtime 比 SOA 安全性早立下基礎，也納入了數十年的大型主機架構經驗，Secure Virtualized Runtime 的開發仍不斷進行中。IBM 持續投入各級網路、伺服器、Hypervisor、程序及儲存體基礎架構的隔離研究與開發，以支援龐大的多租戶環境。

供應虛擬資源可加強安全網域和位置限制。這些虛擬資源必須根據原則分組，而安全配置管理的自動化則有助於確保一致性。

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。IBM Proventia® Virtualized Network Security Platform 是可延伸的虛擬安全平台，可提供入侵防禦、Web 應用程式及網路原則實施等威脅管理功能。

簡化安全控制與防禦的契機

雖然雲端運算會帶來更多安全風險和新的威脅媒介，但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，將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、提供傳輸中及保存資料的預設加密功能，還有透過虛擬儲存體控制資料，這些都是可以改善可靠性及減少資料流失的措施。此外，自動化供應及收回加強型執行時期映像檔的功能也可以減少攻擊範圍，並提高鑑識調查能力。

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。

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**。

讀者也可以參考 *Cloud Security Guidance：IBM Recommendations for the Implementation of Cloud Security* (REDP-4614)。此 IBM 紅皮書提供有關雲端保護、因應威脅及事件管理可靠度的詳細資訊。

您也可以瀏覽下列網站，取得雲端安全性的其他資訊：

IBM 雲端運算：**ibm.com**/cloudcomputing

IBM 企業安全：**ibm.com**/security

IBM 網際網路安全系統：**ibm.com**/services/security

IBMX-Force® 安全警示及建議：xforce.iss.net

此外，IBM 租賃事業部可根據您特定的 IT 需要，提供量身訂做的租賃解決方案。如需優惠價格、彈性付款計劃、貸款以及資產買回與處置的相關資訊，請造訪：**ibm.com**/financing

台灣印製
2009 年 11月

可回收，請回收

TIW14045-USEN-01