新修訂版（第三版）

雲端安全介紹

雲端運算使用案例白皮書

第三版

本書作者

雲端運算使用案例
討論小組

雲端運算使用案例

由「雲端運算使用案例討論小組」製作之白皮書

第 3 版

2010 年 2 月 2 日

參與者：Dustin Amrhein、Patrick Anderson、Andrew de Andrade、Joe Armstrong、Ezhil Arasan B、James Bartlett、Richard Bruklis、Ken Cameron、Reuven Cohen、Tim M. Crawford、Vikas Deolaliker、Andrew Easton、Rodrigo Flores、Gaston Fourcade、Thomas Freund、Valery Herrington、Babak Hosseinzadeh、Steve Hughes、William Jay Huie、Nguyen Quang Hung、Pam Isom、Sam Johnston、Ravi Kulkarni、Anil Kunjunny、Thomas Lukasik、Bob Marcus、Gary Mazzaferro、Craig McClanahan、Meredith Medley、Walt Melo、Andres Monroy-Hernandez、Dirk Nicol、Lisa Noon、Santosh Padhy、Greg Pfister、Thomas Plunkett、Ling Qian、Balu Ramachandran、Jason Reed、German Retana、Bhaskar Prasad Rimal、Dave Russell、Matt F. Rutkowski、Clark Sanford、Krishna Sankar、Alfonso Olias Sanz、Mark B. Sigler、Wil Sinclair、Erik Sliman、Patrick Stingley、Robert Syputa、Doug Tidwell、Kris Walker、Kurt Williams、John M Willis、Yutaka Sasaki、Michael Vesace、Eric Windisch、Pavan Yara 及 Fred Zappert。

本報告由 1,300 名開放網路社群成員完成，創始成員來自「開放雲端宣言」支持者，但很快便廣納全球許多人士，社群包括大小企業、政府機構、顧問及供應商。

報告撰寫期間，宣言中有三項相當重要的原則：一、使用者應共同合作，二、由客戶促進雲端開放，三、盡量使用既有標準。

本文件應持續增補修改，我們將此翻譯版本提供給中文雲端社群，希望擴大對話範圍，報告內容開放討論論壇位於 *http://www.cloudusecases.org*。

希望社群可以運用本報告，爲中文雲端供應者及客戶建立寶貴資源，歡迎您批評指教。

本著作係依據「創用 CC 姓名標示 - 相同方式分享 3.0 Unported 授權條款 (Creative Commons Attribution Share Alike 3.0 Unported License)」提供。

目錄

1 緒論 4
2 定義與分類 6
2.1 雲端運算概念定義 6
2.2 分類 9
2.3 標準與分類的關係 12
2.4 應用程式介面 (API) 13
3 使用案例情況 16
3.1 使用者與雲端 18
3.2 企業、雲端、使用者 19
3.3 企業與雲端 21
3.4 企業、雲端、企業 23
3.5 私有雲 25
3.6 變更雲端供應者 26
3.7 混合雲 28
3.8 交互參照：要求與使用案例 30
4 客戶經驗 32
4.1 客戶經驗：以雲端處理薪資： 32
4.2 客戶經驗：以雲端處理物流及專案管理 33
4.3 客戶經驗：以雲端處理中央政府服務 35
4.4 客戶經驗：以混合雲處理地方政府服務 35
4.5 客戶經驗：天文資料處理 36
5 開發者要求 38
6 安全情況 40
6.1 法規 40
6.2 安全管控 41
6.3 安全聯合模式 42
7 安全使用案例經驗 44
7.1 雲端運算能力 44

(cc) BY-SA

7.2 雲端開發與測試 45
7.3 儲存在雲端 46
7.4 交互參照：安全管控與消費者經驗 47
7.5 交互參照：安全聯合模式與消費者經驗 48
8 結論與建議 49
內容更動 51

關於第三版：第三版新內容重點在於安全，包括技術要求、使用案例及安全模式。細節詳見第 51 頁的「內容更動」。

(cc) BY-SA

1 緒論

「雲端運算使用案例」群組匯集雲端使用者及雲端供應者，雙方共同定義雲端運算常見使用案例情況。這些使用案例情況不僅說明雲端運算的經濟及效能優勢，並針對最廣泛的消費者要求進行分析。

此份白皮書中，重點在於強調雲端運算環境須具備標準化的能力與要求，才能確保互通、易於整合與轉移。設立標準之後，必定能夠在完全不使用封閉性、專利技術的情況下，來實行白皮書內的所有案例。因此，雲端運算必須在開放式環境中演變，降低供應商套牢比例，並增加消費者選擇種類。

使用案例中：

- 提供以客戶經驗爲基礎的實際狀態，供各界討論互通性與標準。
- 明言哪些部分應使用現有標準。
- 讓業界重視「開放式雲端運算」。
- 明言哪些部分需要標準。若特定使用案例目前無法建立，或僅能透過專利應用程式及產品完成，則業界必須定義標準，讓這個案例可行。

使用案例若能明定目標並說明阻礙，即爲進行標準化工作的最佳理由。

「開放雲端宣言」(opencloudmanifesto.org) 堅持雲端運算開放原則。宣言公佈後兩個月內，已有 250 個組織連署支持。本群組活動依據「開放雲端宣言」六原則：

- 雲端供應者必須合作，透過開放合作與善用標準，處理各項應用困難。
- 雲端供應者必須在適當情況應用既有標準。資訊科技產業已大幅投資在既有標準及標準組織，沒有必要重複。
- 若需要制訂新標準或修訂既有標準，必須明確且務實，避免建立過多標準。必須確保標準能鼓勵創新，而非抑制創新。
- 開放雲端的社群工作應依據消費者要求進行，而不只是符合雲端供應者的技術要求，並以消費者實際要求進行測試或驗證。
- 雲端運算標準組織、倡議團體與社群應合作並保持聯繫，確保各種工作不衝突或重複。

(cc) BY-SA

- 雲端供應者不得運用市場地位，強迫消費者使用特定平台及選擇特定供應者。

除白皮書外，本群組亦持續努力落實上述原則。

(cc) BY-SA

2 定義與分類

以下定義與分類是爲綜覽雲端運算概念。不過白皮書重點在於定義雲端應用情況，以及收集實際應用及要求下的使用案例，而非定義雲端運算本身。目的是爲提供明確、值得注意且有用的使用案例情況，而非如何定義或分類這些情況。

2.1 雲端運算概念定義

雲端運算：雲端運算使用無所不在、便利、隨需應變的網路，共享廣大的運算資源（如網絡、伺服器、儲存、應用程式、服務），可透過最少的管理工作及服務供應者互動，快速提供各項服務。（本定義來自 NIST 最新版的「雲端運算工作定義」，由美國政府「國家標準與技術研究院」出版[1]。）

2.1.1 服務模式

NIST 的雲端運算定義共有三種服務模式：

- **軟體即服務 (SaaS)：**消費者使用應用程式，但並不掌控作業系統、硬體或運作的網絡基礎架構。
- **平台即服務 (PaaS)：**消費者使用主機操作應用程式。消費者掌控運作應用程式的環境（也擁有主機部分掌控權），但並不掌控作業系統、硬體或運作的網絡基礎架構。平台通常是應用程式基礎架構。
- **基礎架構即服務 (IaaS)：**消費者使用「基礎運算資源」，如處理能力、儲存空間、網絡元件或中介軟體。消費者能掌控作業系統、儲存空間、已部署的應用程式及網絡元件（如防火牆、負載平衡器等），但並不掌控雲端基礎架構。

2.1.2 部署模型

NIST 定義四種部署模型：

- **公用雲：**簡而言之，公用雲服務可透過網路及第三方服務供應者，開放給客戶使用，「公用」一詞並不一定代表「免費」，但也可能代表免費或相當廉價，公用雲並不表示使用者資料可供任何人查看，公用雲供應者通常會對

[1] NIST 「雲端運算」頁面完整文件請見 http://csrc.nist.gov/groups/SNS/cloud-computing/。文件指出，「這份資料可公開使用，唯需註明 NIST，即可自由複印與翻譯」，本報告有關基本特性、服務模式、應用模式內容源於該文件第 15 版，日期爲 2009 年 8 月 19 日。

(cc) BY-SA

使用者實施使用存取控制機制，公用雲作爲解決方案，既有彈性，又具備成本效益。

- **私有雲：** 私有雲具備許多公用雲環境的優點，例如彈性、適合提供服務，兩者差別在於私有雲服務中，資料與程序皆在組織內管理，且與公用雲服務不同，不會受到網絡頻寬、安全疑慮、法規限制影響；此外，私有雲服務讓供應者及使用者更能掌控雲端基礎架構、改善安全與彈性，因爲使用者與網絡都受到特殊限制。[2]

- **社群雲：**社群雲由眾多利益相仿的組織掌控及使用，例如特定安全要求、共同宗旨等。社群成員共同使用雲端資料及應用程式。

- **混合雲：**混合雲結合公用雲及私有雲，這個模式中，使用者通常將非企業關鍵資訊外包，並在公用雲上處理，但同時掌控企業關鍵服務及資料。[3]

2.1.3 基本特性

NIST 定義雲端運算五項基本特性：

- **高度彈性：**彈性亦即能因應要求調整資源規模大小，對消費者而言，雲端似乎無窮無盡，且能依據需求增減運算能力採購額，這是 NIST 對雲端運算的一大基本定義。

- **計算服務：**計算服務中，雲端服務各層次均由雲端供應者掌控與監管，這對於計費、存取控制、資源優化、處理能力規劃及其他工作相當重要。

- **隨需應變自助服務：**隨需應變與自助代表消費者可自行使用雲端服務，毋需與雲端供應者互動。

- **網路使用無所不在：**網路使用無所不在，亦即雲端供應者服務可隨時在網路取用，且使用者端無論大小，均可透過標準機制使用網路。[4]

- **資源彙整：**資源彙整讓雲端供應者透過多重租賃模式服務消費者，依據消費者要求，來指派或重新指派實體及虛擬資源，在所在地獨立性的概念下，

---

[2] 私有雲可由第三方管理，實體可能暫時外移，並不一定由使用組織管理與經營。

[3] 混合雲爲社群雲所用技術的超集，故兩種應用模式要求合併在第 3 章「混合雲」討論。

[4] 這並不一定代表網路使用，就定義而言，私有雲只能在防火牆內使用，無論網路種類爲何，使用雲端通常不限於特定類別的客戶。

(cc) BY-SA

消費者通常不知道所有資源確切位置，只可能掌握國家、州或資料中心等大範圍的區域地點。[5]

2.1.4 其他名詞

互通性：互通性的重點在於系統之間能否溝通，接收系統必須能瞭解相互傳遞的資訊，在雲端運算世界中，這代表無論供應者有何歧異，程式碼必須可通用於多個雲端供應者之間。[6]

可轉移性：可轉移性意指能夠在另一個環境中，順利執行針對某環境所撰寫的元件或系統，這在雲端運算領域中，包括軟體與硬體、實體與虛擬。

整合：整合意指將元件或系統納入整體系統的程序，雲端型元件及系統之間的整合會受幾個因素影響而變得複雜，包括多重租賃、聯合、政府法規等。

服務等級協議 (SLA)：「服務等級協議」是供應者與消費者之間的協約，載明消費者要求及供應者承諾，通常 SLA 涵蓋項目包括正常運作時間、隱私權、安全、備份程序等。

聯合：聯合意指跨越不同系統匯整資料或身分，聯合可由雲端供應者或雲端仲介者完成。

仲介者：仲介者本身並無雲端資源，而是依據消費者的 SLA 與供應者媒合，消費者並不知道仲介者無法掌控資源。

多重租賃：多重租賃是指在單一硬體上，同時存放不同企業的多個系統、應用程式或資料，多重租賃在多數雲端系統上很常見。

雲端超量：混合雲使用這項雲端超量技術，在私有雲需要時提供後備資源，若私有雲處理能力足以負荷工作量，便不需動用混合雲，若工作量超出私有雲能力，混合雲會自動爲私有雲追加資源。

政策：政策是運作程序的通稱，例如安全政策可能會規定，所有針對特定雲端服務的要求皆須加密。

治理：治理是指透過管控及程序，確保政策得以落實。

---

[5] 在許多情況中，隱私法與其他法規要求，雲端供應者的資源必須在特定位置，雲端供應者與雲端客戶必須合作遵守這些法規。

[6] 互通性、可轉移性與整合定義源於 http://www.testingstandards.co.uk/interop_et_al.htm.

(cc) BY-SA

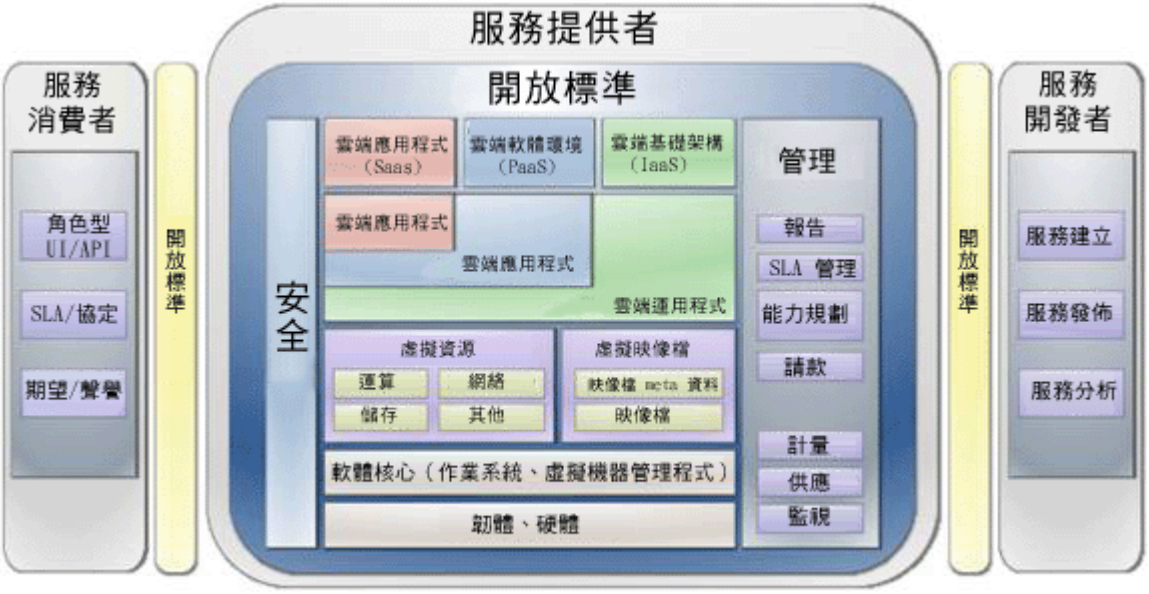
虛擬機器 (VM)：這種檔案（通常稱爲「映像檔」）運作時，在使用者眼中如同實際機器，IaaS 常以虛擬機器映像檔形式呈現，可依需要開關，虛擬機器運作時的變化可永久儲存於硬碟中。

應用程式介面 (API)：API 是種協議，告知開發者如何撰寫程式碼，才能與某種系統互動，API 說明系統運作支援語法，API 會針對每一個作業，載明應傳送給系統什麼資訊、系統會回傳什麼資訊，以及任何可能發生的錯誤情況。

- 可以使用特定程式語言，或使用較中性的格式（如 WSDL 或 IDL），來定義 API。REST 語法通常不具有機器可讀語言，但也能定義 API。
- API 也會包括協定細節 (如 HTTP) 及資料格式（如 JSON 或「XML 綱目」）。
- API 需要人類智慧，才能瞭解資料及作業的語意。機器能發現某方法需要兩個整數爲參數，但必須由人類開發者在無限數字中，找到適合的兩個整數。

2.2 分類

以下圖表定義雲端運算分類：



在這張圖表中，「服務消費者」透過雲端使用服務，「服務提供者」管理雲端基礎架構，「服務開發者」則負責建立服務。（注意：這些角色互動需要開放標準。）以下詳細說明每個角色的功能。

(cc) BY-SA

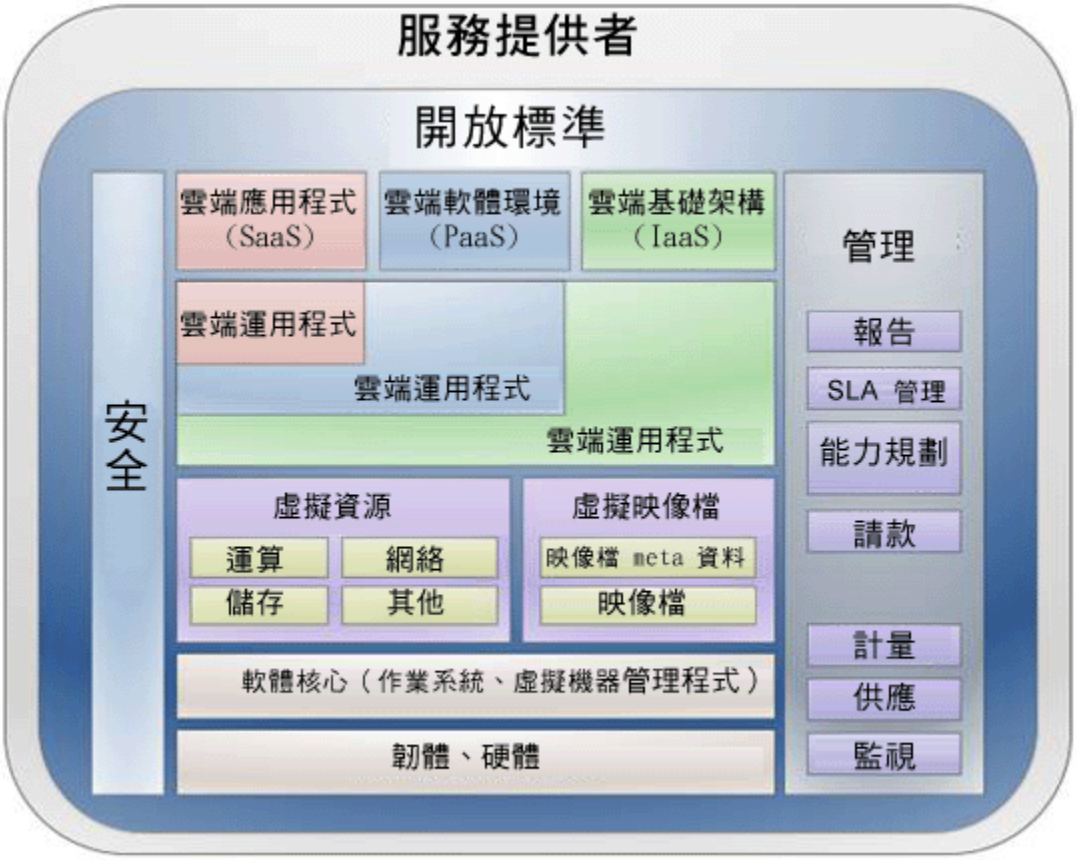
2.2.1 服務消費者

服務消費者爲真正使用服務的使用者或企業，無論是「軟體」、「平台」、「基礎架構即服務」皆然。

根據服務類型及角色不同，消費者會運用不同使用者介面及程式介面，有些使用者介面外觀與其他應用程式無異，消費者使用應用程式時，不需瞭解雲端運算；其他使用者介面提供管理功能，如開關虛擬機器、管理雲端儲存空間等，消費者撰寫應用程式碼時，根據應用程式內容，使用不同程式介面。

消費者也會接觸到 SLA 及其他協定，通常此部分會由消費者及供應者協商，消費者期望及供應者聲譽在協商過程中很重要。

2.2.2 服務供應者



(cc) BY-SA

服務供應者提供服務給消費者，實際項目則依服務種類有別：

- 就「軟體即服務」而言，供應者安裝、管理及維護軟體，供應者不一定擁有軟體運作所需的實體基礎架構，消費者均無法接觸基礎架構，只能使用應用程式。

- 就「平台即服務」而言，供應者爲平台管理雲端基礎架構（通常爲特定應用程式類型的基礎架構），消費者的應用程式無法觸及平台背後基礎架構。

- 就「基礎架構即服務」而言，供應者維護儲存空間、資料庫、訊息佇列或其他中介軟體，或是虛擬機器所在的主機環境，消費者使用時，將服務當成硬碟、資料庫、訊息佇列或機器，但無法觸及其管理基礎架構。

在服務供應者圖表中，最底層爲基礎韌體及硬體，上一層則爲軟體核心，爲管理雲端基礎架構的作業系統或虛擬機器管理程式，虛擬資源與映像檔包括各種基本雲端運算服務，例如處理能力、儲存空間及中介軟體，由虛擬機器管理程式掌控的虛擬映像檔，包括映像檔本身及管理所需的 meta 資料。

管理層面對服務供應者的作業很重要，在基礎層次中，管理者需要一套計量方式，來決定使用者的身分及權限、安排資源給消費者、追蹤系統狀態及資源。

在較高層次中，管理工作包括攤平成本、確保可滿足消費者要求、SLA 管理（確保履行雙方協議內容）、通報高層等。

服務供應者運作須考量各層面的安全（許多安全要求面向超出本報告討論範圍），也要符合開放標準，完善標準將簡化供應者運作內容，並確保與其他供應者的互通性。

(cc) BY-SA

2.2.3 服務開發者

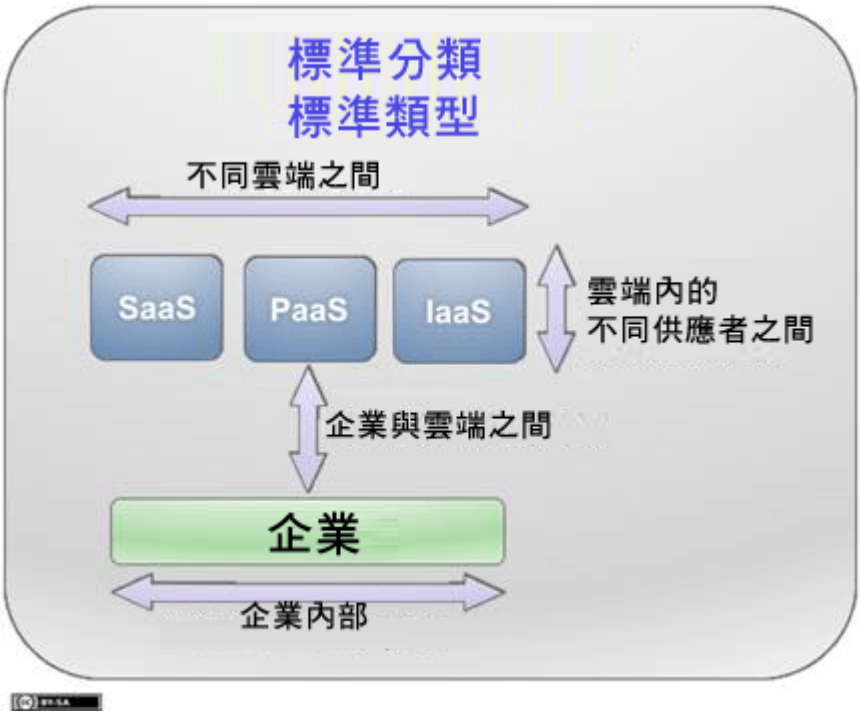
服務開發者建立、發佈及監控雲端服務，通常屬於「商務營運」應用程式，透過 SaaS 模式直接送至使用者手中，而在 IaaS 及 PaaS 層次撰寫的應用程式，也會受到 SaaS 開發者及雲端供應者採用。

建立服務的開發環境各有不同，若開發者在設計 SaaS 應用程式，很可能會為雲端供應者管理的環境撰寫程式碼，在這種情況下，發佈服務會將其部署在雲端供應者基礎架構中。

在服務設計過程中，分析內容包括以遠端除錯作為測試，再發佈給消費者使用，服務一旦發佈後，分析數據能讓開發者監控服務效能，並進行必要修改。

2.3 標準與分類的關係

標準共有四種影響雲端使用案例的方式，包括各種類型的雲端服務內部、不同雲端服務之間、企業與雲端之間、企業私有雲內部。



(cc) BY-SA

2.3.1 各類雲端服務標準

隨著雲端運算日益普及，應用程式可能使用不同類型的雲端服務，例如雲端儲存服務、雲端訊息佇列，並管理（啓動/關閉/監控）在雲端運作的虛擬機器，定義不同服務如何合作的標準應有其價值。

2.3.2 各類雲端服務內部標準

在每一種雲端服務（IaaS、PaaS、SaaS）中，開放標準能避免供應者套牢。

對 IaaS 而言，與雲端資料庫合作的 API 若有標準，即可使用不同供應者的資料，共同 API 讓使用者可自由轉移至其他雲端資料庫供應者，但不需經過大幅變動，也會讓新資料來源與現有應用程式更容易整合。儲存、訊息佇列或 MapReduce 等其他雲端基礎架構的共同 API 亦有相似優點，資料與資料交換共同格式亦然。而在虛擬機器方面，共同虛擬機器格式非常重要，使用者應可取得由某雲端供應者建置及部署的虛擬機器，且不必做任何改變，即可將其部署至不同雲端供應者。

對 PaaS 而言，雲端提供的許多平台皆爲應用程式基礎架構，這些基礎架構通常提供一般服務，如使用者介面、儲存與資料庫，但只能透過基礎架構下的 API 取用。

對 SaaS 而言，開放標準適用於應用程式層次，多數標準並非針對雲端運算，故這些標準不在本報告討論範圍內，例如雲端文書處理應用程式應支援文件可轉移性標準，這項要求與應用程式是否在雲端運作無關。

2.3.3 雲端與企業之間的標準

縱然擁有雲端運算，Java EE 等企業架構並不會消失，若建立標準，明確定義企業應用程式如何與各項資源（如雲端資料庫、雲端訊息佇列）互動，就可在變化最小的情況下使用雲端服務，企業最大挑戰在於，如何將雲端運算融入現有架構及發展規劃中。

2.3.4 企業內部標準

企業內部標準取決於互通性、可審核性、安全與管理等要求，並以企業及雲端之間的標準爲基礎，企業會與私有雲、公用雲、混合雲互動。

2.4 應用程式介面 (API)

建立雲端運算解決方案的主要機制，即爲雲端供應者所提供的 API，雲端 API 運作分爲四個層次，且可區分爲五個基本類別。

(cc) BY-SA

2.4.1 API 層次

API 共有四種層次，開發者在每一層次關注的任務及資料結構不同。

層次 1 – 網絡：在這個層次，開發者直接撰寫網絡格式的要求，若服務以 REST 爲基礎，開發者能創造適當的 HTTP 標頭資訊、建立要求內容、並開啓連結服務的 HTTP，REST 服務回覆資料時，會附上 HTTP 回應碼，因爲許多 REST 服務很直接，故在這個層次撰寫程式碼時相對有效率。

若服務以 SOAP 爲基礎，開發者建立 SOAP 信封、加上適當 SOAP 標頭，再將資料內容加入主體，SOAP 服務回覆時，是以 SOAP 信封裝載要求結果，使用 SOAP 服務時，必須分析信封內的 XML 內容，因此會使用較高層次的 API 來呼叫多數 SOAP 服務。

層次 2 – 特定語言工具箱：開發者在這個層次使用特定語言工具箱，以配合 SOAP 或 REST 的要求，雖然開發者仍專注於網絡內部的資料格式與結構，許多細節已交由工具箱處理，例如處理回應程式碼、計算簽章等。

層次 3 – 特定服務工具箱：開發者使用較高層次的工具箱，並與特定服務配合，開發者在此層次能夠專注於企業物件與企業程序，開發者若專注於組織相關的資料與程序，而非網絡協定，效能會高出許多。

層次 4 – 非特定服務工具箱：這是最高層次的 API，開發者使用多重雲端運算供應者的共同介面，和層次 3 相同，開發者專注於企業目標及企業程序，但與層次 3 不同的是，層次 4 開發者不需擔心雲端服務項目，使用非特定服務工具箱撰寫的應用程式，應該不需更動或只更動一小部分，就能轉移至不同的雲端供應者（見第 26 頁「變更雲端供應者」）。

2.4.2 API 類別

應用程式介面可分爲五個類別：

類別 1 - 一般程式設計：一般程式設計介面包括 C#、PHP、Java 等，此類在雲端運算並無特殊之處。

類別 2 - 部署：將程式部署在雲端的程式介面，除了雲端運算特殊封裝技術外，還包括 .Net 組件及 EAR/WAR 檔等傳統封裝機制。

類別 3 - 雲端服務：程式介面需與雲端服務配合，如前一節所述，雲端服務應用程式介面並不一定與服務種類有關，這些 API 又可細分爲幾類：雲端儲存服務、雲端資料庫、雲端訊息佇列、其他雲端服務，開發者使用雲端服務 API 撰寫程式碼時，都知道自己正使用雲端服務。

(cc) BY-SA

類別 4 - 映像檔與基礎架構管理：程式介面要管理虛擬機器映像檔及基礎架構細節，與映像檔相關的 API 支援上傳、啓動部署、停止佈署、重新啓動部署、及刪除映像檔等功能，基礎架構管理 API 掌控各種細節，如防火牆、節點管理、網絡管理、負載平衡。

類別 5 - 內部介面：指在雲端基礎架構不同區塊之間的內部程式介面，若要變更雲端架構儲存服務供應者，則須使用此類 API。

2.4.3 開發者角色

討論開發者要求之前，先瞭解開發者所扮演的各個角色，將會有所幫助，API 與雲端服務要求會因角色不同而受到影響，以下是本報告論及的角色，以及他們使用的 API 分類：

用戶端應用程式開發者：爲使用者撰寫雲端用戶端應用程式，這些開發者使用雲端服務 API（類別 3）。

應用程式開發者：撰寫使用雲端的傳統應用程式，這些開發者使用一般 API（類別 1），以及雲端服務 API（類別 3）。

部署者：包裝、部署與維護使用雲端的應用程式，生命週期循環在此亦爲一項因素，這些開發者選擇部署、雲端服務與映像檔服務類的 API（類別 2、3、4）。

管理者：在不同層面接觸應用程式，包括部署及基礎架構管理，這些開發者使用類別 2、3、4 的 API。

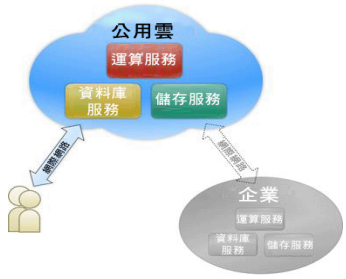
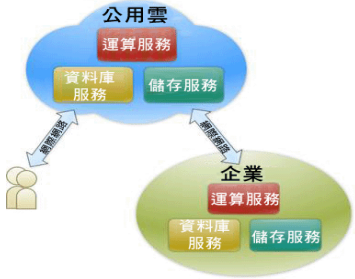
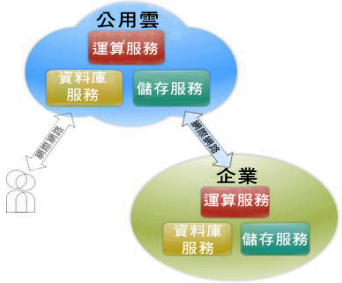
雲端供應者：雲端供應者會運用其雲端供應項目下的基礎架構，這些開發者使用類別 5 的 API。

(cc) BY-SA

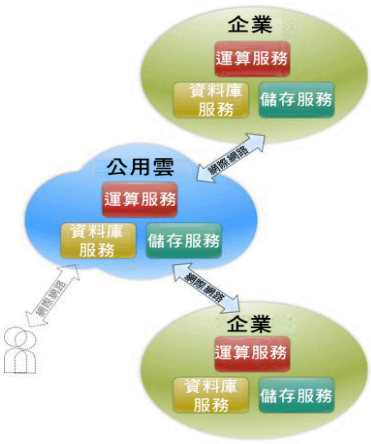
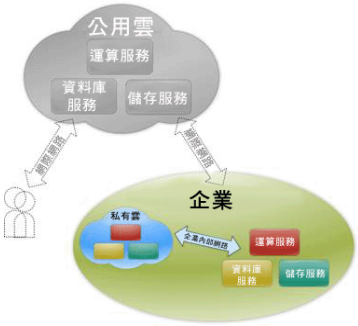
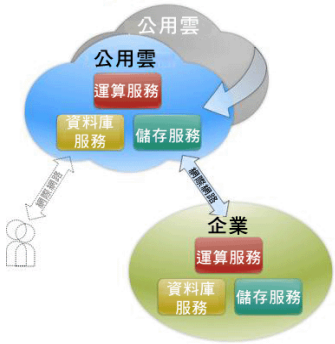
3 使用案例情況

「企業雲端使用」情況說明最典型的雲端使用案例，但未盡述雲端環境中的所有實際情形。

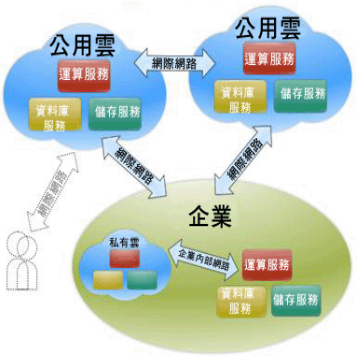
本章節圖片有些共同元素，若某一元素在該使用案例中不存在，就會變成灰色與虛線，例如「私有雲」使用案例中，並無「使用者」或「公用雲」角色，故只有「企業」爲彩色。

使用者與雲端	使用者使用的雲端應用程式	
企業、雲端、使用者	在公用雲上執行、由員工及消費者使用的應用程式	
企業與雲端	與內部資訊科技能力整合的雲端應用程式	

(cc) BY-SA

企業、雲端、企業	在公用雲上執行的雲端應用程式，且與其他應用程式互通（供應鏈）	
私有雲	組織在組織防火牆內管理的雲端。	
變更雲端供應者	使用雲端服務的組織決定變更雲端供應者，或增加其他雲端供應者。	

(cc) BY-SA

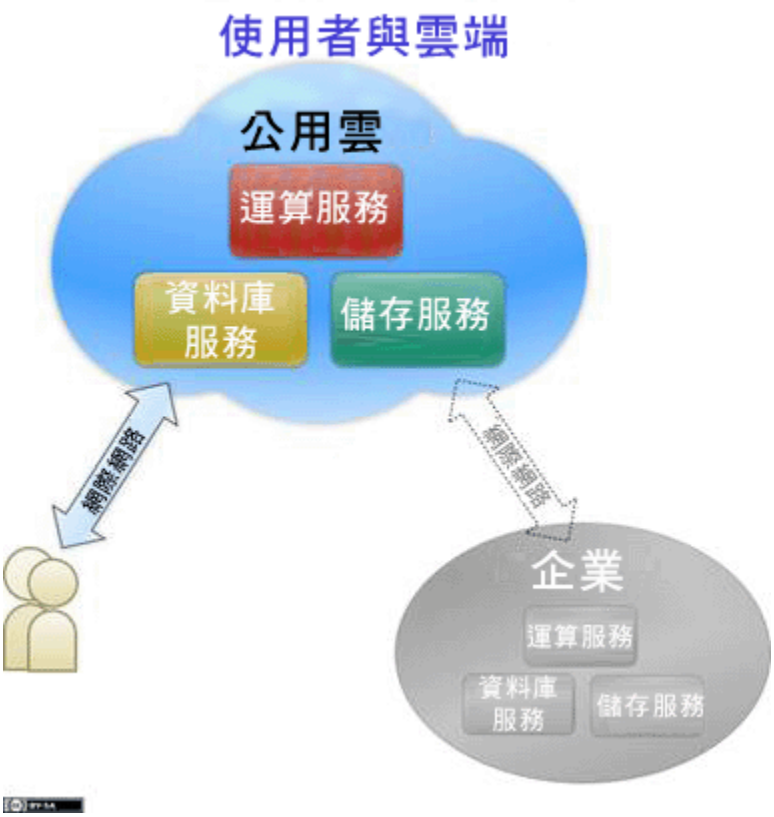
混合雲	由雲端仲介者結合多個雲端，匯整資料、應用程式、使用者身分、安全及其他細節。	

3.1 使用者與雲端

在此情況中，使用者能使用雲端資料或應用程式，此類常見應用程式包括電子郵件及社交網站，Gmail、Facebook 或 LinkedIn 使用者可透過瀏覽器或其他裝置，使用這項應用程式及資料，使用者通常只需記住密碼，其餘資料皆在雲端儲存及管理。

最重要的是，使用者完全不需瞭解基礎架構運作方式，只要能使用網路，就能取得資料。

(cc) BY-SA



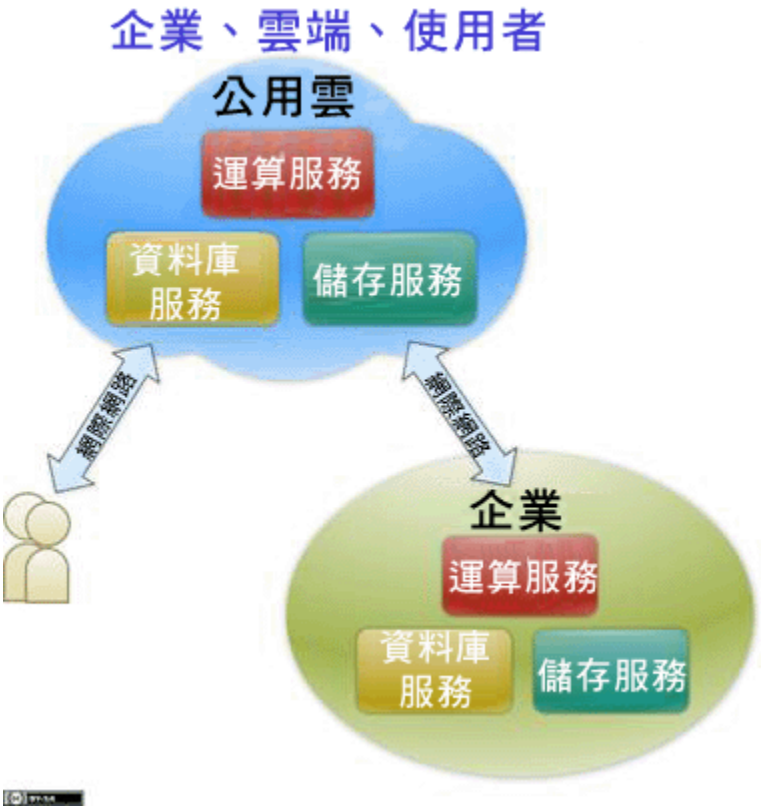
3.1.1 要求

- **身分**：雲端服務必須鑑別使用者。
- **開放型用戶端**：使用雲端服務不應限制於特定平台或技術。.
- **安全**：安全（包括隱私權）是所有使用案例的共同要求，不過個別案例細節差異甚鉅，雲端運算詳細安全討論超出本報告處理範疇。
- **SLA**：雖然使用者的服務等級協議通常比企業版簡化許多，雲端供應者仍須言明服務保障。

3.2 企業、雲端、使用者

在此情況中，企業利用雲端傳遞資料與服務給使用者，使用者與企業互動時，企業透過雲端取得並（或）操縱資料，再將結果送回給使用者，使用者可能是企業內部人士，也可能是外部客戶。

(cc) BY-SA



3.2.1 要求

- **身分**：雲端服務必須鑑別使用者。
- **開放型用戶端**：使用雲端服務不應限定特定平台或技術。
- **聯合身分**：除了使用者所需的基本身分之外，企業使用者也可能會擁有企業身分，在理想的情況下，企業使用者只需管理單一身分，而基礎架構會自行聯合其他雲端服務所需身分。
- **位置資訊**：取決於企業代表使用者管理何種資訊，而法律上可能對資料儲存的實體伺服器位置有所限制，雖然在雲端運算理想中，使用者不必知道實體基礎架構細節，但這項要求有其必要，除非雲端供應者提供 API，標示提供雲端服務的硬體實際位置，否則許多應用程式無法移至雲端。
- **計量與監管**：所有雲端服務的成本掌控、退款及預備，都必須接受計量與監管。
- **管理與治理**：公用雲供應者讓設立帳戶與使用雲端服務變得相當容易，但同時也造成風險，企業裡的個人會將雲端服務挪為私用，因此需要管理虛擬機器，以及管理儲存、資料庫及訊息佇列等雲端服務，以追蹤人們使用何種服

(cc) BY-SA

務。

治理是爲確保使用者無論在何處使用雲端運算，皆會遵守政策及政府法規。其他治理要求則依產業及地區有別。

- **安全**：相較於單一使用者，任何牽涉企業的使用案例中，安全要求都比較複雜，若要依據愈先進的企業使用案例，就得採用愈先進的安全要求。

- **虛擬機器共同檔案格式**：虛擬機器應可在不同雲端供應者平台之間自由轉移，此要求的解決方案還必須考量到，雲端供應者的虛擬機器儲存方式各異。

- **雲端儲存與中介軟體共同 API**：企業使用案例需要共同 API，以使用雲端儲存服務、雲端資料庫，以及訊息佇列等其他雲端中介軟體服務。

  若爲特定供應者的雲端服務撰寫程式碼，則會限制企業使用該供應者系統，且無法利用雲端運算提供的部分財務優點及彈性。

- **資料與應用程式聯合**：企業應用程式需要結合多重雲端來源的資料，且需要整合不同雲端裡的應用程式活動。

- **SLA 與評比**：除了使用者要求的基本 SLA 之外，企業依 SLA 簽署合約時，也需要評比表現的標準方式，必須明確定義雲端供應者服務項目，並明定如何衡量是否履約。（SLA 對雲端安全另有其他意涵，更多 SLA、審核與監管討論請見第六章。）

- **生命週期管理**：企業必須能夠管理應用程式與文件生命週期，包括應用程式不同版本，以及保留與銷毀資料，如何探索資料對許多組織是一大問題，而若無法取得特定資料，則會牽涉到巨大法律責任，此外，除保留資料外，有時企業會在某些時刻希望確保銷毀資料。

3.3 企業與雲端

本案例與企業爲內部程序使用雲端服務有關，因爲企業擁有最多掌控權，所以這可能是雲端運算早期最常見的使用案例。

(cc) BY-SA

在此情況中，企業使用雲端服務輔助所需資源：

- 使用雲端儲存將鮮少使用的資料備份或存檔
- 使用雲端虛擬機器，增加網路處理器以應付高峰期（並在高峰期後關閉虛擬機器）
- 使用雲端應用程式（SaaS）處理企業業務（電子郵件、日曆、客戶關係管理等）
- 使用雲端資料庫加入應用程式處理程序與夥伴、政府機構共享資料庫時很方便

3.3.1 要求

「企業與雲端」使用案例基本要求，大抵和「企業、雲端、使用者」使用案例相同，包括**開放型用戶端、聯合身分、位置資訊、計量與監管、管理與治理、安全、虛擬機器共同檔案格式、雲端儲存與中介軟體共同 API、資料與應用程式聯合、SLA、生命週期管理**等。

此項案例其他要求包括：

(cc) BY-SA

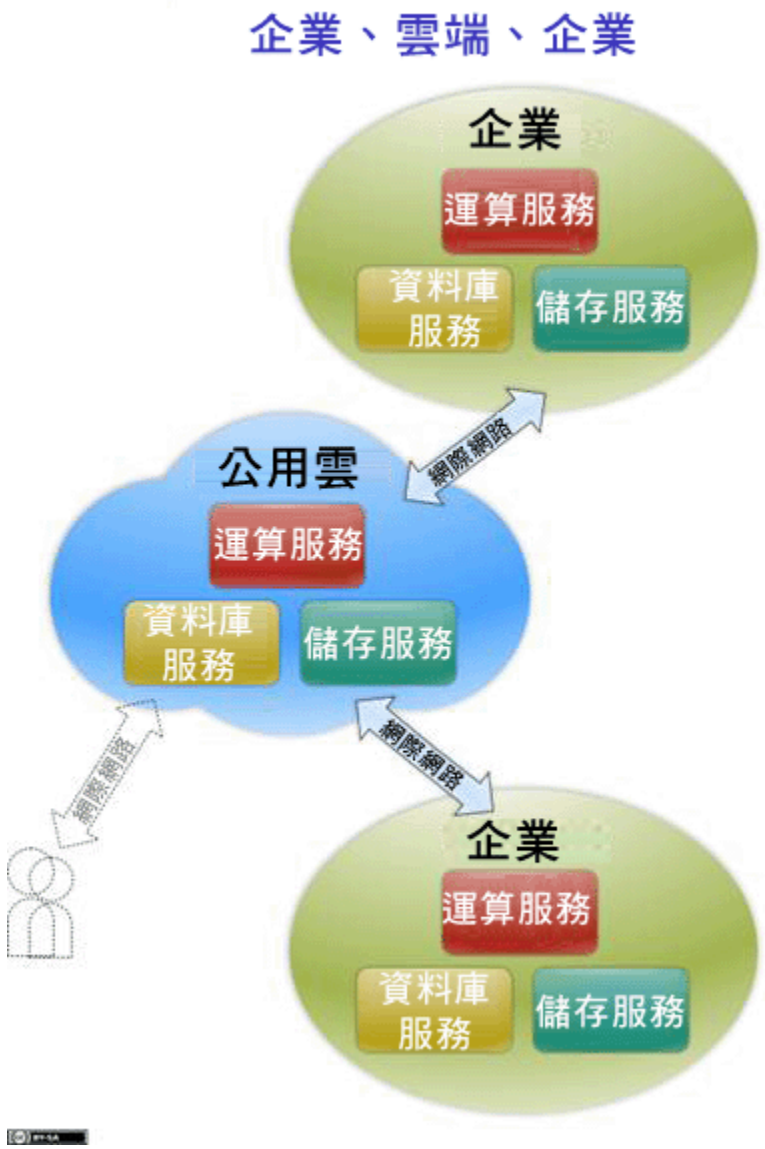
- **部署**：建立虛擬機器映像檔，並於必要時部署在雲端，此作法應該很容易完成，建立虛擬機器映像檔後，雖然不同供應者的相關儲存機制不同，仍可在不同供應者之間轉移，將應用程式部署至雲端也要盡量直接。

- **特定產業的標準與協定**：許多企業之間的雲端運算解決方案，將會使用 RosettaNet 或 OAGIS 等既有標準，個別應用程式及各個產業適用標準各異。

3.4 企業、雲端、企業

這個案例共有兩家企業使用同一個雲端，重點在於將資源置於雲端，讓企業應用程式可互通，供應鏈是這項使用案例最顯著的範例。

(cc) BY-SA



3.4.1 要求

「企業、雲端、企業」使用案例基本要求，大抵和「企業與雲端」使用案例相同，包括**身分、開放型用戶端、聯合身分、位置資訊、計量與監管、管理與治理、安全、產業特定標準、儲存與中介軟體共同 API、資料與應用程式聯合、SLA、生命週期管理**等。

此項案例其他要求包括：

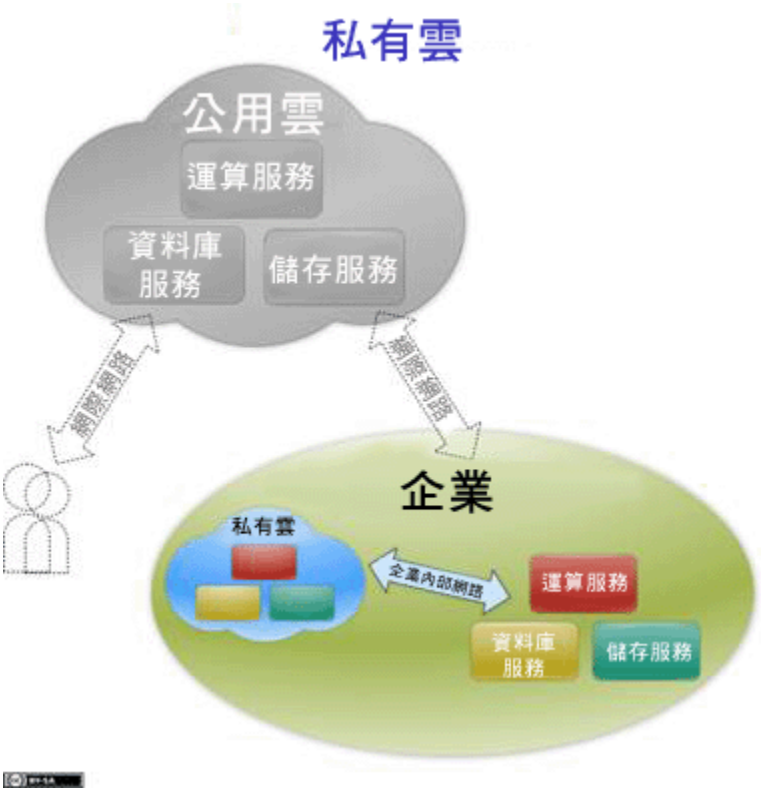
- **即時交換資訊**：如果不同企業要共享應用程式及資料，則即時交換資訊非常重要，若兩家企業使用同一套雲端管理應用程式、虛擬機器、中介軟體或儲存空間，任何一方若有更動都必須相互告知。

(cc) BY-SA

- ***互通性***：因爲多家企業參與，互通性是基本條件。

3.5 私有雲

「私有雲」案例與其他案例不同，因爲私有雲設於企業*內部*。這樣的做法對於大型企業相當有幫助，例如，薪資部門在每個月 15 日及 30 日工作量大增，需要足夠運算能力來消化工作，但其他時間工作量則減少許多，若設立私有雲，企業各部門可共享運算能力，薪資部門即可在需要時增加必要運算能力，而其他部門亦然，並可節省大量企業成本。



3.5.1 要求

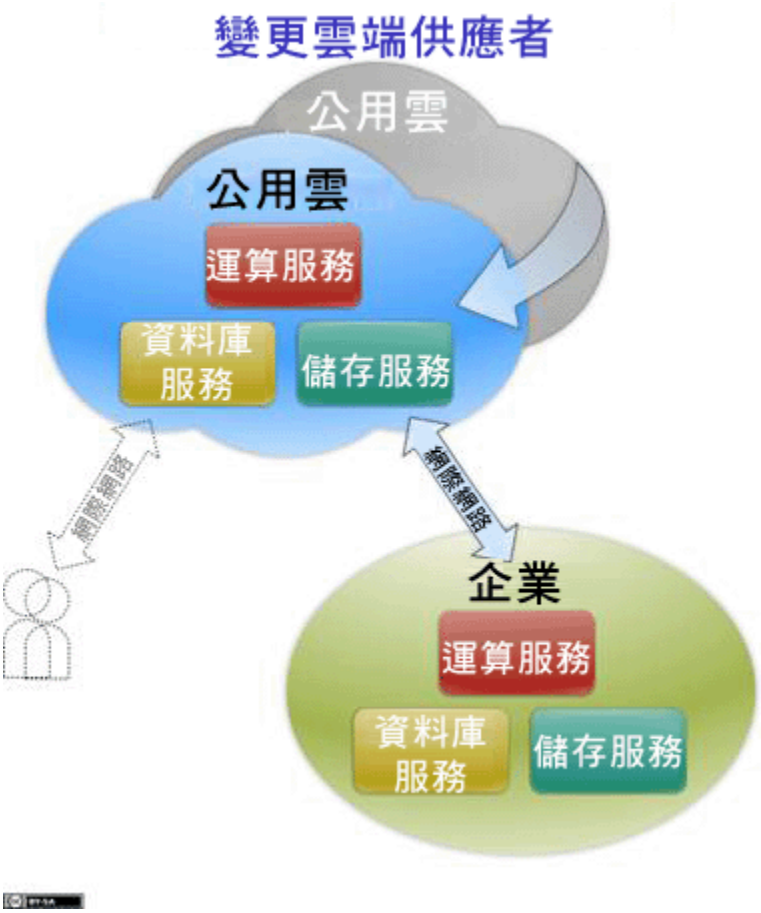
私有雲使用案例基本要求包括**開放型用戶端、計量與監管、管理與治理、安全、部署、互動性、虛擬機器共同格式、SLA** 等。

請注意，私有雲不需要身分、聯合身分、位置資訊、交易、產業標準、雲端中介軟體共同 API 及生命週期管理，在許多情況下，消費者必須使用私有雲，才能擺脫位置資訊疑慮，私有雲亦可免除身分管理、標準與共同 API 等要求。

(cc) BY-SA

3.6 變更雲端供應者

這個案例是與另一個雲端供應者合作，可能是新增供應者，或是取代既有供應者，這種情況適用於本報告討論的其他所有案例中，保持開放及標準化的一大優點，即爲新增或變更供應者時，不需經歷大幅變動。



以下四種情況的個別要求稍有差異，整體而言，變更雲端供應者需要**開放型用戶端、位置資訊、安全、SLA、虛擬機器共同檔案格式、雲端儲存與中介軟體共同 API**，各項要求細節討論如下：

3.6.1 情況一：變更 SaaS 供應者

在此情況中，雲端客戶變更 SaaS 供應者，新舊供應者提供同一套應用程式（客戶關係管理、會計、文書處理等），先前建立的文件與資料，應能匯入新供應者的軟體中，有時客戶也許得交互使用兩家供應者。

(cc) BY-SA

3.6.1.1 要求

- **特定產業標準**：在兩項應用程式移轉文件及資料時，雙方必須能支援共有格式，格式取決於應用程式類型。

  在某些案例中，也需要符合不同應用程式類型的標準應用程式介面。

重點在於，這些要求並非特別針對雲端運算，將文件從 Zoho 移轉至 Google Docs 的標準，就和移轉 Microsoft Office 的文件至 OpenOffice 相同。

3.6.2 情況二：變更中介軟體供應者

在此情況中，雲端客戶變更雲端中介軟體供應者，既有資料、要求、訊息佇列與應用程式，必須能在兩方供應者之間匯出與匯入。[7]

3.6.2.1 要求

- **特定產業標準**：在兩項應用程式移轉文件及資料時，雙方必須能支援共有格式，格式取決於應用程式類型。

- **雲端中介軟體共同 API**：包括所有今日雲端服務支援的功能（如雲端資料庫、雲端訊息佇列及其他中介軟體），並包括連結、建立與刪除資料庫與表格的 API。

  雲端資料庫供應者藉由部分限制，讓產品更具彈性，限制查詢大批資料組時佔用大量處理資源的可能性（例如，部分雲端資料庫禁止各圖表之間連結，有些不支援實際資料庫綱目）。這些限制會導致難易變更雲端資料庫供應者，對於使用關係模型建立的應用程式更是如此。

  訊息佇列等其他中介軟體服務較相似，故較容易找到交集。

3.6.3 情況三：變更雲端儲存供應者

在此情況中，雲端客戶變更雲端儲存供應者。

[7] 因爲雲端儲存相當熱門，雲端中介軟體（資料庫、訊息佇列、Map Reduce ）與雲端儲存雖同樣爲 PaaS，一般認爲兩種情況有別。

(cc) BY-SA

3.6.3.1 要求

- **雲端儲存共同 API**：變更雲端儲存系統時，讀寫資料的程序碼變更應愈少愈好，變更應限制在配置碼中，以 JDBC 應用程式爲例，URL 格式及驅動程式名稱在各資料庫供應者各異，但與資料庫互動的程式碼完全一樣。

3.6.4 情況四：變更虛擬機器主機

在此情況中，雲端客戶希望取得建於某一雲端供應者系統的虛擬機器，並在另一個系統上執行。

3.6.4.1 要求

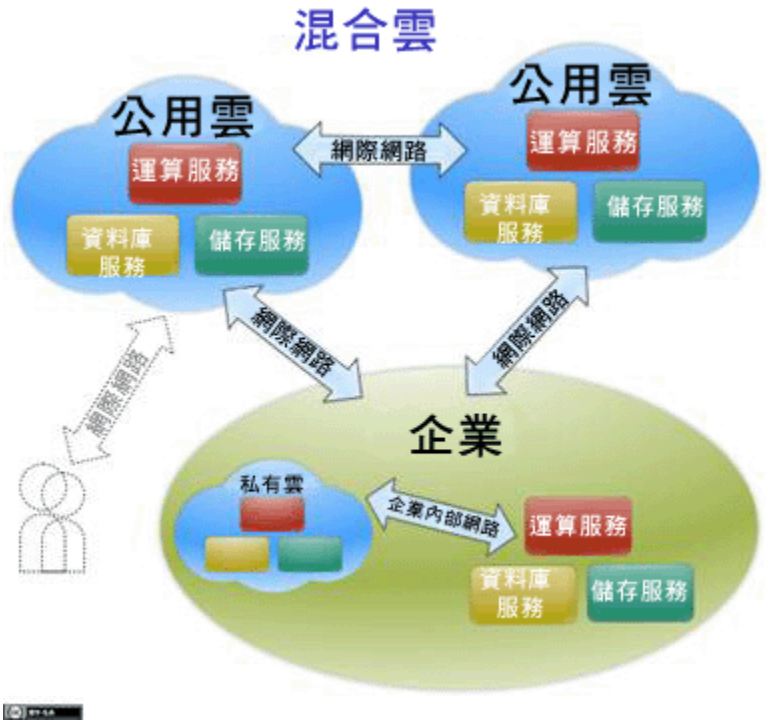
- **虛擬機器共同格式**：虛擬機器格式應適用於所有作業系統。

  假設虛擬機器是在 Windows 或 Linux 等作業系統中執行，表示虛擬機器使用者在建立雲端虛擬機器前已選擇平台，因此對於虛擬機器內運作的軟體沒有特定的雲端要求。

3.7 混合雲

這個案例包括公用雲、私有雲一同合作，混合雲可由聯合雲端供應者（結合自身與其他供應者的資源）提供，仲介者亦可提供混合雲，差別在於仲介者手中並未掌控任何雲端資源，混合雲供應者必須依據消費者要求來管理雲端資源。

(cc) BY-SA



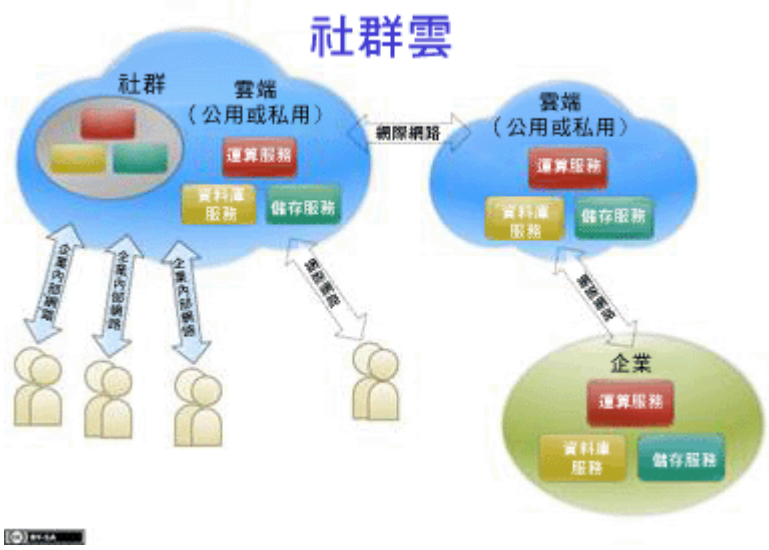
請注意，對混合雲消費者而言，這個使用案例與前述「使用者與雲端」無異，使用者不知道混合雲供應者實際操作模式。

3.7.1 要求

- 包括所有前述案例要求（除「**即時交換資訊**」一項），尤其是**安全、資料與應用程式聯合、互通性**。
- **SLA**：用來表示 SLA 的標準機器可讀格式，讓混合雲供應者可依據消費者要求，在無人為干預情況下選擇資源。

如第 2 章所述，社群雲的要求是混合雲要求的子集，社群雲具有企業共享的基礎架構，而這些企業擁有共同目標。社群雲基礎架構如下圖：

(cc) BY-SA



請注意，社群與社群雲是透過內部網絡進行溝通，這個部分可能是 VPN，但並非透過公開網路使用。

3.8 交互參照：要求與使用案例

以下表格整理要求與使用案例的關係：

要求	使用者與雲端	企業、雲端、使用者	企業與雲端	企業、雲端、企業	私有雲	變更雲端供應者	混合雲
身分	✓	✓		✓			✓
開放型用戶端	✓	✓	✓	✓	✓	✓	✓
聯合身分		✓	✓	✓			✓
位置資訊		✓	✓	✓		✓	✓
計量與監管		✓	✓	✓	✓		✓
管理與治理		✓	✓	✓	✓		✓
安全	✓	✓	✓	✓	✓	✓	✓

(cc) BY-SA

要求	使用者與雲端	企業、雲端、使用者	企業與雲端	企業、雲端、企業	私有雲	變更雲端供應者	混合雲
部署			✓		✓		✓
即時交換資訊				✓			
互通性				✓			✓
產業特定標準			✓	✓			✓
虛擬機器映像檔格式		✓	✓	✓	✓	✓	✓
雲端儲存 API		✓	✓	✓		✓	✓
雲端資料庫 API		✓	✓	✓		✓	✓
雲端中介軟體 API		✓	✓	✓		✓	✓
資料與應用程式聯合		✓	✓	✓			✓
SLA	✓	✓	✓	✓	✓	✓	✓
生命週期管理		✓	✓	✓			✓

(cc) BY-SA

4 客戶經驗

本章描述使用案例中的客戶經驗，以下為客戶經驗摘要：

客戶經驗	解決客戶問題	要求與能力	適用案例
薪資處理	• 處理時間縮短 • 硬體要求減少 • 提高未來擴張彈性	IaaS（虛擬機器）、雲端儲存	企業與雲端
物流及專案管理	• 處理時間縮短 • 免除人工 • 更新與簡化開發環境	PaaS（應用程式基礎架構）、雲端儲存	企業、雲端、使用者
中央政府	• 整合資訊科技專業 • 硬體要求減少	IaaS、PaaS	私有雲
地方政府	• 整合資訊科技專業 • 硬體要求減少	IaaS、PaaS	混合雲
天文資料處理	• 硬體開銷大幅減少（處理能力及儲存） • 能源成本大幅減少 • 行政簡化	IaaS（虛擬機器）、雲端儲存	企業、雲端、使用者

4.1 客戶經驗：以雲端處理薪資：

4.1.1 第 3 章適用的使用案例：

企業與雲端

4.1.2 客戶經驗：

在此經驗中，業主使用兩台伺服器處理複雜耗時的薪資業務，組織決定嘗試運用雲端處理此業務是否可行，現有系統為分散式應用程式，故轉移工作應該相對直接。

應用程式過去使用 SQL 資料庫處理員工資料，業主並未為雲端資料庫服務重新撰寫應用程式，而在虛擬機器上配置資料庫伺服器，資料庫伺服器自雲端儲存系統取

(cc) BY-SA

得資料後，建立關係表格，由於原始資料庫規模龐大，故運用工具挑選薪資處理必要資訊，經挑選的資訊轉移至雲端儲存服務，再交由資料庫伺服器使用。

將薪資應用程式部署到同時運作的四台虛擬機器，四台機器則與管理資料庫伺服器的虛擬機器配合，除了改為使用置入資料庫伺服器的虛擬主機，薪資應用程式其餘配置不變。

4.1.3 解決客戶問題：

雲端版本的應用程式裡，薪資處理時間縮短八成，除此之外，先前用來處理薪資的兩部伺服器，如今可移作其他用途，且雲端版本更具彈性，對組織擴張後將成為一大優勢。

4.1.4 要求與能力

案例採用虛擬機器及雲端儲存（IaaS）兩項雲端服務，薪資應用程式不需調整，僅需部署在虛擬機器上，因為原始應用程式使用的是關聯式資料庫，為避免改變資料結構，並避免讓應用程式使用雲端資料庫，因而將關聯式資料庫部署在雲端。

唯一使用的 API 為 S3 雲端儲存 API。

4.1.5 可轉移性顧慮：

薪資應用程式在 Fedora 及 Java 1.5 上運作，故雲端供應者平台只要支援 Fedora，即可運作而不需改變，若新雲端儲存供應者不支援處理薪資的 S3 API，轉移應用程式可能會有問題，最終會使得應用程式改用雲端資料庫變得極為困難，此外，假若雲端資料庫不支援關係模式，情況將更加複雜。

4.2 客戶經驗：以雲端處理物流及專案管理

4.2.1 第 3 章適用的使用案例：

企業、雲端、使用者

4.2.2 客戶經驗

一家小型營造商約有 20 名行政管理員工，希望能管理資源、優化專案排程及追蹤工作成本，該公司要求相當明確，因為既有系統並不適用，故結合 Quickbooks 及試算表，但該系統既無彈性，又嚴重浪費人力資源。

解決方案為建立客製化應用程式，所有企業運作模式由客戶決定，應用程式資料由「 Google 應用程式引擎」（GAE）資料庫軟體負責，這套軟體除了 RDF 圖表之

(cc) BY-SA

外，並無其他圖表，不過仍有一套 RDF-OWL 爲本體，客戶運用本體驗證資料後，再提供給使用者，或回送至 GAE。

資料運作是利用應用程式專用的 REST HTTP 協定來與資料庫通訊，在伺服器管理的序列系統中，資料庫軟體會維護應用程式專用的 RDF 圖表，並依據使用特定資料序列的應用程式要求，個別維護每項序列的安全。只要使用這套系統，無論多少應用程式皆可使用同一套資料庫軟體，而不需爲每項應用程式撰寫新碼源。

資料從 Quickbooks SQL 伺服器轉移至 GAE 的資料庫軟體，試算表則使用相容的一次性轉移指令碼，再上傳至 GAE 資料庫軟體，因爲資料組很小，使用本地資源即可輕易運作。

用戶端應用程式仍留在本地資料庫軟體，其中包含資料最近期改變的子集。應用程式的 REST 架構，讓 HTTP 的內建快取支援能自動將更動傳遞至主要資料庫軟體，再交給客戶。除了使用資料子集的效能優點外，這項設計也簡化安全程序，若用戶端應用程式不需存取某些欄位或記錄，該部分的資料儲存庫永遠不會離開伺服器。

4.2.3 解決客戶問題：

資料從效能低落的軟體及試算表巨集，轉移至雲端系統，結果資料庫軟體可用在各種應用程式上，讓未來開發與維護簡單許多。

雖然原有應用程式基礎架構仍在使用中，應用程式卻不再仰賴試算表分析及操控資料，由於不必再維護試算表，大幅節省成本，此外，也不需再以人工方式剪貼資料，不但可避免耗時工作，並可降低錯誤機率。

4.2.4 要求與能力：

這項雲端服務使用 GAS，爲一 PaaS 程式，提供資料庫支援，結合 REST API 與雲端資料庫軟體後，相較於傳統關聯式資料庫建立的應用程式，新程式更具彈性。

4.2.5 可轉移性顧慮：

應用程式使用 GAE 及 BigTable 資料庫，後者爲一稀疏、分散、持續、多維度排序的地圖，將非正規化置於正規化之前，藉以達到彈性，這和其他資料庫軟體大不相同，也需要從更根本來思考應用程式開發過程，若在較傳統的資料庫軟體上運算應用程式，將需要大幅改變應用程式架構。

(cc) BY-SA

4.3 客戶經驗：以雲端處理中央政府服務

4.3.1 第 3 章適用的使用案例：

私有雲

4.3.2 客戶經驗：

日本政府各部會基礎架構下共有數千個伺服器，中央政府決定建立「霞關」私有雲，以提供安全的核心基礎架構運作政府應用程式。

現有後勤系統（例如薪資、會計、人事管理等）將在虛擬化之後置入私有雲中，電子採購等部分客務系統也將虛擬化置入公用雲，但不在本案例討論範圍內，最終目標是要減少整體成本，去除累贅系統，並免除各部會行政要求。

4.3.3 解決客戶問題：

混合雲可解決三項問題：降低成本、減少耗能、精簡資訊科技人事。

4.3.4 要求與能力：

雲端基礎架構將建立在日本電訊公司的私有網絡上，由於隱私及安全是主要考量，私有雲爲必要模式，多種個人資料依法不得儲存於日本以外的伺服器。

4.3.5 可轉移性顧慮：

因爲政府自建私有雲，可轉移性不是問題，政府不打算將核心應用程式及資料，從私有雲移轉至公用雲。

4.4 客戶經驗：以混合雲處理地方政府服務

4.4.1 第 3 章適用的使用案例：

混合雲

4.4.2 客戶經驗：

日本全國地方政府超過 1,800 個，都各有伺服器及資訊科技員工，日本內閣霞關雲端的第二項目標，即爲提供混合雲環境，除了內閣雲端之外，中央政府決定依行政區將地方政府分組，每個縣均建立私有雲，並連結至內閣的混合雲，內部工作及部分資料將存於各縣私有雲，其他資料則儲存在當地，各地現有系統都將虛擬化，存放在霞關雲端的主機內。

(cc) BY-SA

4.4.3 解決客戶問題：

混合雲解決三項問題：降低成本、減少耗能、精簡資訊科技人事。

4.4.4 要求與能力：

隱私與安全在此案例格外重要，日本法律禁止某些資料儲存於非地方政府伺服器中，故不能將應用程式與資料移往霞關雲端，由於部分處理工作得在地方政府基礎架構進行，故匯整混合雲裡的應用程式及資料即爲關鍵工作。

4.4.5 可轉移性顧慮：

如同前一項客戶經驗，可轉移性不是問題，因爲政府自建私有雲，政府不打算將核心應用程式及資料，從私有雲移轉至公用雲。

4.5 客戶經驗：天文資料處理

4.5.1 第 3 章適用的使用案例：

使用者與雲端

4.5.2 客戶經驗：

「蓋亞」[8] 爲「歐洲太空總署」任務，職責爲研究銀河系裡十億顆星球，將在五年內監測每顆目標星球約 70 次，並精準丈量位置、距離、移動與亮度變化，預計將發現數十萬顆新物體，例如太陽系外星球、棕矮星等。

這項任務將收集大量需分析資料，「歐洲太空總署」決定爲此設計一套雲端系統原型，希望藉此瞭解使用雲端運算處理大量資料時，會面臨的技術及財務層面。

原型系統內包括科學資料，以及過往發揮計算功能的白板，由內部開發分散式運算基礎架構，則用來執行工作與處理資料，這個基礎架構是爲處理「全球多次天體測量方案」（AGIS）而設計，這個程序在匯整之前，已多次處理過這些資料。

進行處理工作時，每個工作站都會從資料庫取得工作說明、取得資料、經過處理，再將結果回送給中級伺服器，更新資料供下次使用。

原型系統評估 200 萬顆星球共五年的資料，只是真正計畫需處理資料的一小部分。原型系統每百分鐘重複 24 次，相當於連續運作 20 台虛擬機器 40 小時。而

[8] 該計畫總覽請見 http://www.esa.int/esaSC/120377_index_0_m.html。

(cc) BY-SA

在十億星計畫中，將分析一億顆主要星球六年，需要 20 台虛擬機器運作 16,200 小時

爲評量雲端方案彈性，原型系統亦進行第二次測試，使用 120 台高中央處理器的特大虛擬機器，每台虛擬機器可處理 12 筆資料，故同時共可處理 1,440 筆資料。

4.5.3 解決客戶問題：

雲端解決方案預估成本不到內部方案的一半，這份估算書中，未計算內部方案所需的額外電力或系統管理成本，故實際節省金額更高，資料儲存也將以雲端模式解決。

在第二次試驗中，發現並解決 SQL 序列幾項表現問題，以及資料庫鎖爭奪問題，這些問題在現有內部系統中無法找到，原型系統讓組織能在落實之前，找出並解決表現與彈性問題。

4.5.4 要求與能力：

原型系統使用虛擬機器處理 AGIS 軟體及資料庫，資料庫是在虛擬機器內運作的傳統資料庫，爲一全套關聯式資料庫，並非雲端資料庫服務；儲存方面則使用五套雲端儲存系統（各 100 GB），附加在資料庫伺服器上。

4.5.5 可轉移性顧慮：

所有虛擬機器皆使用標準作業系統，所有軟體均非爲雲端系統設計，這項應用程式的顧慮在於，將虛擬機器映像檔搬遷至其他雲端供應者時，能否不需重建或重新處理這些映像檔。

(cc) BY-SA

5 開發者要求

開發者要求遍及所有使用案例及消費者情景，爲簡化討論過程，所有開發者要求如下：

- **快取**：程式設計工具箱若支援雲端資源快取，將提升雲端應用程式表現，開發者需要 API 連結快取，也可能需要 API 將特定物件或資料置入快取。
- **集中記錄**：無論開發者角色或撰寫應用程式種類，所有開發者均一致要求記錄功能，API 應支援撰寫記錄、檢視條目、建立記錄與開關記錄檔案。
- **資料庫**：開發者需要使用雲端資料庫，雲端資料庫設計差異甚鉅（有些涉及圖表與關係，有些完全無關），故開發者撰寫雲端應用程式時，會依據個別程式要求選擇雲端資料庫供應者，資料庫 API 必須支援基本的 CRUD 運算。
- **身分管理**：開發者需要管理身分，以最簡單的例子而言，需要鑑別任何使用者證明屬實，應用程式若與多項資料來源及應用程式合作，開發者便需要串連使用者身分，聯合身分管理系統能製作證明，讓使用者可使用特定服務，縱然服務與使用者不知道對方亦然，身分管理 API 應適當地快取及刪除憑證。
- **端到端訊息**：開發者需要 API 張貼訊息至佇列，並消費這些訊息，API 必須讓開發者得窺訊息（檢視訊息內容，但不會消耗訊息）。
- **發佈/訂閱訊息**：開發者需要 API 以處理訊息佇列系統主題，API 應讓開發者張貼並收取主題訊息。
- **原始計算/工件處理**：開發者需要 API 以應付大量處理工作，例如 Hadoop 形式的資料探勘，API 應容許開發者開關、監管及暫停處理工作。
- **階段作業管理**：尤其在雲端環境裡，管理使用者階段作業相當重要，若出現機器錯誤，雲端基礎架構必須具有彈性，故縱然某一節點失靈，仍可維持階段作業管理，API 階段作業必須讓人們易於取用或操控使用者階段作業。
- **服務探索**：開發者需要探索何種雲端服務可用，雲端服務應透過服務種類探索，由 API 依據不同服務種類，提供另一層適當功能。
- **SLA**：開發者使用服務探索時，需要自動方式決定所獲的服務政策，擁有此類 API 後，開發者能撰寫應用程式在雲端服務之間互通，並選擇最符合 SLA 標準的項目。

(cc) BY-SA

- **儲存**：開發者需要使用雲端儲存服務，API 必須提供儲存及喚回資料與 meta 資料的能力。

以下表格對照 2.4.2 節討論的五類 API 與開發者要求。

開發者要求	一般程式設計	部署	雲端服務	映像檔與基礎架構管理	內部介面
快取				✓	✓
集中記錄	✓	✓	✓	✓	✓
資料庫			✓		✓
身分管理		✓	✓	✓	✓
端到端訊息			✓		
發佈/訂閱訊息			✓		
原始計算/工件處理			✓	✓	✓
服務探索		✓	✓	✓	✓
階段作業管理	✓		✓		
SLA	✓	✓	✓	✓	✓
儲存		✓	✓	✓	✓

(cc) BY-SA

6 安全情況

無論在雲端與否，安全這個重要問題俯拾即是，此章節是為突顯，建置者與開發者移往雲端時，所應考量的安全議題。

有一項重點必須謹記在心，雲端並未帶來任何新的安全威脅或問題，以安全而言，雲端運算整體是個理想使用案例，可彰顯無論雲端部署模型為何，安全基礎架構一致、透明與標準多麼重要。隨著企業轉移至雲端，或在雲端建立解決方案，擁有一致性安全模型儼然十分重要，除非如此做，才能簡化開發工作，並避免供應商套牢，節省企業資訊科技投資。

從雲端運算考量安全，最大差異在於企業失去掌控權，而非任何技術困難，在內部應用程式中，限制敏感資料及應用程式使用很重要，雲端應用程式存取控制同樣重要，但安全基礎架構、平台與應用程式直接受到雲端供應者掌控。

以下是本章節討論安全議題的次序：

- **法規**：法規並非技術問題，但一定要處理，法規所影響的安全要求凌駕於功能要求。
- **安全管控**：雖然消費者也許需要所有安全管控措施，但消費者仍需懷疑，雲端供應者基礎架構是否有能力提供所有安全相關保障。
- **安全聯合模式**：為落實安全管控，需要不同的聯合模式，雲端供應者應透過現有安全標準提供聯合模式。

上述資訊為本章節使用者經驗討論定調。

6.1 法規

使用雲端運算時，除了所有技術問題，還有法規相關的殘酷現實（報告先前已曾提及規範問題，但在安全脈絡下需要更多討論）。

由於各種原因，世界各國政府均關切雲端運算使用問題，許多國家訂定嚴格隱私權法律，禁止特定資料儲存於國外實體機器中，組織或組織高層若違法將處重刑，任何組織若將敏感資料儲存於雲端，必須證明雲端供應者儲存資料時，並未存放在特定地區以外的實體伺服器內。

除政府機構之外，許多貿易及產業團體亦建立規範，這些規範或許無法律效力，但仍代表最佳範例。

(cc) BY-SA

類似情況也發生在雲端運算的應用程式上，若虛擬機器在雲端上運作，在虛擬機器上運作的應用程式是否會接觸到敏感資料？這是個許多國家尚未觸及的灰色地帶，不過未來將會出現新法律與新規範。

遵守法律規範凌駕其他要求，新法或許要求組織將資源用於更改應用程式基礎架構，而非增加特性，「資訊長」辦公室必須管理這些變化，並時時注意新法規動態。

6.2 安全管控

適當管控是維護系統安全的必要條件，以下章節介紹多項使用案例及個別安全要求，案例與管控要求之間關係說明如下。

安全管控	內容說明
資產管理	必須能夠管理組成雲端基礎架構的所有硬體、網絡及軟體資產（實體與虛擬皆然），包括對實體或網絡資產取用負責，並配合審核及監管。
加密：金鑰及憑證管理	任何安全系統都需要一套基礎架構，以落實並管理加密金鑰與憑證，包括落實標準加密功能與服務，以支持靜止及流通資訊安全。
資料/儲存安全	必須以加密格式儲存資料，此外，有些消費者資料儲存必須與其他消費者資料區隔。
終端安全	消費者必須能確保雲端資料終端安全，包括藉由網絡協定及設備種類限制終端。
事件審核與通報	消費者必須能得知雲端各項事件資料，尤其是系統錯誤與安全疏漏等，得知活動資訊包括瞭解歷史事件、通報新事件，雲端供應者若未及時通報事件，將嚴重損及聲譽。
身分、角色、存取控制與屬性	必須以一致、機器可讀的方式，定義身分、角色、權利及其他個人及服務屬性，才能有效落實存取控制，並維護雲端資源安全政策。
網絡安全	必須在開關、路由器、封包等方面確保網絡流量安全，IP 程式本身也應安全。
安全政策	必須定義、解決與落實安全政策，以一致、機器可讀方式，支援存取控制、資源分配及其他決定，此種定義方法必須健全，才能讓 SLA 及授權自動生效。

(cc) BY-SA

安全管控	內容說明
服務自動化	必須以自動化方管理及分析安全管控流及程序，以支援安全監管審核，包括通報任何違反安全政策或客戶憑證協議的事件。
工作量及服務管理	必須依據安全政策及客戶憑證協議，以配置、部署及監控服務。

以下是可應用於各項管控的部分標準：

安全管控	相關標準
加密：金鑰及憑證管理	**KMIP**：OASIS「金鑰管理互通性協定」(http://www.oasis-open.org/committees/kmip/)
資料/儲存安全	**IEEE P1619**：由 IEEE「儲存安全工作組」開發 (https://siswg.net/)
身分、角色、存取控制與屬性	**SAML**：OASIS「安全判定標示語言」(http://saml.xml.org/)
身分、角色、存取控制與屬性	**X.509 憑證** ：ITU「公開金鑰與屬性基礎架構建議」內容 (http://www.itu.int/rec/T-REC-X.509)
安全政策	**XACML**：OASIS「可延伸存取控制標示語言」(http://www.oasis-open.org/committees/xacml/)
工作量及服務管理	**SPML**：OASIS「服務供應標示語言」(http://www.oasis-open.org/committees/provision/)

6.3 安全聯合模式

聯合亦即讓多項獨立資源如同單一資源運作，雲端運算本身即爲聯合資源，故在單一雲端運算解決方案中，許多資產、身分、配置及其他細節必須聯合，才能發揮效果。

前一節提到的要求透過以下聯合模式落實：

- **信任**：指雙方在鑑別機構下建立信任關係的能力，鑑別機構能夠交換證明（通常爲 X.509 憑證），並以此確保訊息安全及建立已簽署的安全記號（通常爲 SAML），信任聯合是所有其他安全聯合模式的基礎。

- **身分管理**：藉由使用者證明（帳號、密碼、文件）憑證身分，並回覆符合使用者的已簽署安全記號，服務提供者若信任身分提供者，縱然毫不認識使用者，亦可使用安全記號，開放適當權限給使用者。

(cc) BY-SA

- **使用管理**：能夠制定政策（通常為 XACML）檢視安全記號，以管理雲端資源使用情況，使用資源會受到多個因素掌控，例如限制僅特定角色使用者可使用資源、只能在特定協定中使用、限制使用時段等。

- **單一登入/登出**：根據可信任機構憑證匯整登入資訊，由於已鑑別使用者已具有特定角色，單一登入功能讓使用者只需登入某一應用程式，即可使用其他信任相同機構的其他應用程式。單一登出模式亦然，在許多情況下，使用者若自某一應用程式登出，就必須同時登出其他應用程式，單一登入模式需以身分管理模式為基礎才能執行。

- **審核及監管**：可收集散佈在混合雲等多重網域內的審核及監管資料，聯合審核為必要工作，可確保並記錄活動符合 SLA 及法規要求。

- **配置管理**：結合服務、應用程式及虛擬機器的配置資料，包括使用政策及跨網域授權資訊。

因為既有安全規範已應用在雲端運算，供應者應延用現有標準作為聯合模式。

(cc) BY-SA

7 安全使用案例經驗

本章節描述消費者使用雲端運算與符合安全要求的經驗，定義要求與模式後，即可觀察實地情況，呈現雲端安全如何落實，案例涵蓋眾多應用程式種類、部署模型、模式與角色。

7.1 雲端運算能力

7.1.1 客戶經驗：

有一家保險公司擁有一套索賠應用程式，用來收集被保險人資料及所受損失情況。颶風預計將襲擊美國墨西哥灣地區，可能造成重大財產損失，導致索賠案件大增，也大幅提高企業資訊科技基礎架構負荷。

該公司決定與公用雲提供者合作，使用虛擬機器應付預期要求，企業必須掌控自有系統與雲端虛擬機器的使用權，只限公司合格經理人取用，此外，企業也要安全地將雲端申請案的資料送回企業防火牆內，而雲端供應者必須確保虛擬機器一旦關閉後，應用程式與資料記錄會徹底消失。

7.1.2 解決客戶問題：

使用公用雲後，讓企業能處理異常大增的工作量。透過添購、維護、供電與冷卻額外系統來處理可能面臨的巨大工作量，並不符合成本效益，該公司內部已有運算能力，可應付日常維運，故可在所需時間自動增加運算能力。

7.1.3 要求與掌控：

本案例要求及相關掌控內容包括：

要求	掌控
限制特定人士可使用影片	• 身分、角色、存取控制與屬性 • 資產管理 • 網絡安全
虛擬機器關閉時，所有應用程式及資料記錄必須刪除	• 工作量及服務管理

7.1.4 聯合模式：

信任、使用管理、配置管理

(cc) BY-SA

7.1.5 角色

索賠核算員、保險代理人、審核員

7.2 雲端開發與測試

7.2.1 客戶經驗：

網路零售業者需要開發一套新的 Web 2.0 店面應用程式，但不想增加資訊科技部門與現有資源負擔，故選擇一家雲端供應者，提供雲端開發環境，儲存開發工具及來源碼，由另一家雲端供應者提供測試環境，讓新應用程式可與各種機器及大量工作互動。

因爲運用兩家提供者區隔開發與測試，故雙方聯合非常重要。

7.2.2 解決客戶問題：

在開發者眼中，使用雲端開發工具後，就不必在每位開發者的電腦裡安裝、配置及管理工具，工具更新也只需在雲端進行一次，所有開發者就自動取得同一版本的工具。

產品建置速度會加快，大規模建置工作可運用雲端提供者的基礎架構彈性，且在雲端開發時，能取用雲端資料庫裡最新版來源碼。

就測試而言，由於公司從傳統介面轉移至 Web 2.0 介面，對伺服器的額外負擔無法預估。相較於靜態網頁，Web 2.0 介面與伺服器互動更頻繁，故在雲端測試新應用程式時，測試團體能計算新介面產生的衝擊。

在雲端進行新應用程式壓力測試容易許多，若測試團隊希望瞭解，若要求每秒自 500 台不同機器傳來，應用程式表現如何，雲端運算可承受這種試驗，由於虛擬機器映像檔各異，要用不同機器（作業系統、版本、協定等）測試應用程式也很簡單，即使測試團隊想將規模增至千台或萬台機器，在雲端測試的成本效能也遠低於內部基礎架構測試。

7.2.3 要求與掌控：

本案例要求及相關掌控內容包括：:

要求	掌控
在單一中央位置安裝並維護開發者工具	• 資產管理
虛擬機器關閉時，所有應用程式及資料記錄必須刪除	• 工作量及服務管理

(cc) BY-SA

要求	掌控
單次登入通行開發雲與測試雲	• 加密 • 終端安全 • 身分、角色、存取控制與屬性 • 網絡安全
限制使用來源碼及測試計畫人士	• 資產管理 • 身分、角色、存取控制與屬性
開發與測試必須自動開關虛擬機器	• 服務自動化
開發與測試必須通報虛擬機器使用及表現數據	• 事件審核與通報

7.2.4 聯合模式：

信任、身分管理、使用管理、單一登入、審核與監管、配置管理

7.2.5 角色：

開發者、測試者、管理者、審核員

7.3 儲存在雲端

7.3.1 客戶經驗：

一家金融投資公司將爲經理人及分公司推出新投資產品，已製作數段影片，向經理人及分公司說明新產品特長，由於影片檔案很大，必須具備隨需應變瀏覽方式，故儲存在雲端可減少企業基礎架構要求，但影片觀看者身分需嚴格限制，爲商業競爭考量，只有合格經理人能觀看影片，更重要的限制是，在產品推出前夕，影片及產品細節必須保密。

該公司決定採用公用雲儲存供應者，負責安全管控及影片播放，雲端解決方案必須具備使用存取控制機制，以落實該公司對影片的安全政策。

7.3.2 解決客戶問題：

使用公用雲儲存服務後，讓消費者能處理大量資料檔案及頻寬要求，但不會增加資料中心的實體資源。然而，因爲政府法規與組織要求，安全格外重要，公用雲儲存供應者若無法保證監管功能，無論效能如何、價格或彈性高低，都不能採用。

(cc) BY-SA

7.3.3 要求與掌控：

本案例要求及相關掌控內容包括：

要求	掌控
限制特定人士可使用應用程式	• 身分、角色、存取控制與屬性 • 資產管理 • 網絡安全 • 政策
儲存在雲端的資料必須安全	• 加密 • 資料/儲存安全
儲存在雲端的資料必須轉移至企業防火牆內	• 加密 • 資料/儲存安全 • 終端安全 • 網絡安全

7.3.4 聯合模式：

信任、身分管理、使用管理、審核與監管

7.3.5 角色：

影片製作單位、企業經理人、企業分公司、審核員、法規單位

7.4 交互參照：安全管控與消費者經驗

以下表格整理安全管控與消費者經驗的關係：

安全管控	雲端運算能力	雲端開發與測試	儲存在雲端
資產管理	✓	✓	✓
加密：金鑰與憑證管理		✓	✓
資料/儲存安全			✓
終端安全		✓	✓
活動審核與通報		✓	
身分、角色、存取控制	✓	✓	✓

(cc) BY-SA

與屬性			
網絡安全	✓		✓
政策			✓
服務自動化		✓	
工作量與服務管理	✓	✓	

7.5 交互參照：安全聯合模式與消費者經驗

以下表格整理安全聯合模式與消費者經驗的關係：:

安全聯合模式	雲端運算能力	雲端開發與測試	儲存在雲端
信任	✓	✓	✓
身分管理		✓	✓
使用管理	✓	✓	✓
單一登入		✓	
審核與監管		✓	✓
配置管理	✓	✓	

(cc) BY-SA

8 結論與建議

雲端運算搭配也建基於許多產業趨勢，包括虛擬化、服務導向基礎架構、Web 2.0 等，故許多報告所提到的要求中，已有許多標準存在，我們在進步的同時，也會透過社群合作，確立既有標準能符合消費者要求、運用已在進步的標準，並找出如何彌補既有標準的缺口。

本報告由 900 名開放網路社群成員完成，創始成員來自「開放雲端宣言」支持者，但很快便廣納全球許多人士，社群包括大小企業、政府機構、顧問及供應商。

報告撰寫期間，宣言中有三項相當重要的原則：一、使用者應共同合作，二、由客戶促進雲端開放，三、盡量使用既有標準，本報告證明這些原則可行，也將成爲未來後續工作核心。

各項案例反映出以下消費者常見要求：

- **共同虛擬機器格式、資料格式與 API** ：虛擬機器、資料與應用程式應該不需更動，就可直接在不同雲端供應者之間轉移。
- **雲端管理**：雲端運算若要有效，必須具備服務管理、治理、計算、監控、聯合身分、SLA 與檢查程式、資料與應用程式聯合、部署、生命週期管理，這些要求請見第 3 章。
- **安全**：安全對雲端運算至關重要，不過安全要求依據應用程式及資料類別差異甚鉅。
- **位置資訊**：若要瞭解雲端基礎架構實體主機位置，其中一項方式就是透過各種政府法規限制。

消費者應用報告內各項案例時，應該不需使用任何封閉式專利解決方案，導致受供應者種種限制。

開發者要求大抵可區分爲兩大類型：

- **服務相關的 API** ：API 要求若與資料庫、訊息（端到端、發佈/訂閱）、原始運算能力、儲存相關，都直接涉及雲端服務。
- **支援型 API** ：API 必須對快取、記錄、身分管理、服務探索、階段作業管理及 SLA 有所要求，才能有效運用雲端服務。

開發者者應用報告內各項案例時，應該不需使用任何封閉式專利解決方案，導致受供應者種種限制。

(cc) BY-SA

消費者將資料與應用程式移往雲端時，安全仍是最大考量，然而，雲端運算並未新增任何安全議題，一切皆源於整體資訊科技安全。使用雲端的主要顧慮，在於落實安全政策如今牽涉第三方，因爲失去掌控權，雲端供應者透明化更顯得重要。相關內容討論突顯出，雲端供應者必須確保安全管控、聯合模式與標準。

在雲端運算各個面向中，因爲現有標準加上要求，我們必須確保標準能一致且廣泛落實，現有標準若不符要求，就必須定義與落實這些標準，這份由社群完成的報告希望作爲參考，以供建立真正開放的雲端運算環境。

(cc) BY-SA

內容更動

2009 年 10 月 30 日第二版：

- 新增開發者要求段落。第 2.4 節加入 API 不同層次、API 類別、開發者角色內容。第二版新內容重點，在於開發者及其要求。
- 在文中適當處變更措詞，以「彈性」取代「可擴張」一詞。
- 更新第 2.1 節的分類討論，以反映 NIST 對雲端運算定義變化。
- 更新第 4.4 節消費者經驗。
- 擴大討論部署一致性及虛擬機器共同格式，包括雲端供應者儲存虛擬機器不同方式。

2010 年 2 月 2 日第三版

- 考量安全因素，在第 3.2.1 節「服務等級協議」有小幅變動。
- 增加第六節安全情況與要求，增加第七節安全使用案例。

(cc) BY-SA