# IBM Application Security on Cloud

本使用條款 ("ToU") 由本 IBM 使用條款 - SaaS 特定供應項目條款（「SaaS 特定供應項目條款」）及標題為 IBM 使用條款 - 一般條款（「一般條款」）的文件構成，該文件可於下列 URL 取得：http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/。

如互有牴觸者，前項「SaaS 特定供應項目條款」較「一般條款」優先適用。一經訂購、存取或使用 IBM SaaS，即表示「客戶」同意本使用條款。

「使用條款」受所適用之「IBM International Passport Advantage 合約」、「IBM International Passport Advantage Express 合約」或 IBM International Agreement for Selected IBM SaaS Offerings（視適用情況而定）（以下稱為「合約」）之規範，「合約」與「使用條款」共同構成本完整合約。

## 1. IBM SaaS

下列 IBM SaaS 供應項目受前項 SaaS 特定供應項目條款之規範：

- IBM Application Security Analyzer
- IBM Application Security on Cloud Consulting Services

## 2. 計費度量

IBM SaaS 係依「交易文件」所定下列其中一項計費度量而銷售：

a. **「工作」**- 是獲得 IBM SaaS 的一種計量單位。「工作」是 IBM SaaS 中的一個物件，該物件不可再被分割並代表一個處理程序，內含其所有子處理程序。「客戶」應在其「權利證明書 (PoE)」或「交易文件」中所指定的計量期間，取得足夠涵蓋 IBM SaaS 所處理或管理的「工作」總數的授權數。

b. **「應用程式實例」**- 是獲得 IBM SaaS 的一種計量單位。每一個連接至 IBM SaaS 的「應用程式」實例都需要「應用程式實例」授權。 若「應用程式」具有多重元件，且各元件均提供不同用途及/或使用者基本程式，並可連接至 IBM SaaS 或由其管理，則各該元件分別視為不同「應用程式」。此外，「應用程式」之測試、開發、暫置及正式作業環境分別視為不同「應用程式」實例，故各需一份授權。單一環境中之多個「應用程式實例」分別視為不同「應用程式」實例，皆各應備有一份授權。「客戶」應在其「權利證明書」或「交易文件」中所指定的計量期間，取得足夠涵蓋連接至 IBM SaaS 之「應用程式實例」數量之授權數。

   基於本 IBM SaaS 之目的：

   - 適用於「動態測試」：可透過公用或私有 URL 定址之網站。每一「應用程式實例」於單一網域均授權使用頁面數量高達 1,000 頁之網站。
   - 適用於「靜態測試」：可於單一程式設計語言中執行之程式碼單元。每一「應用程式實例」均授權使用高達 1,000,000 行之掃描程式碼單元。
   - 適用於「行動式測試」：可於行動式裝置上執行之二位元碼單元。不同行動式平台（例如：iOS 及 Android）包含不同「應用程式實例」。

c. **「實例」**- 是獲得 IBM SaaS 的一種計量單位。一「實例」是對一 IBM SaaS 特定配置的存取權。「客戶」應在其「權利證明書 (PoE)」或「交易文件」中所指定的計量期間，取得足夠讓 IBM SaaS 的每一個實例可供存取及使用的授權數。

   各「實例」授權，其所執行「工作」之數量或「應用程式實例」（已連接的應用程式）之數量均未受限制，但於任何特定時間同時執行之「工作」，其數量不得逾 30 個。

d. **「約定」**- 是取得服務所需的一種計量單位。一個「約定」(Engagement) 係由有關 IBM SaaS 的專業及/或訓練服務組成。「客戶」應取得足夠的授權數，才能涵蓋每一個「約定」。

## 3. 計費及付款

IBM SaaS 的付款金額明訂於「交易文件」中。

### 3.1 未足月費用

「交易文件」所定未足月費用得按比例計算之。

### 3.2 超額使用計費

若「客戶」在計量期間內的 IBM SaaS 實際使用情形超出「權利證明書」載明之授權數量，則針對超額使用部分將依「交易文件」之規定向「客戶」收取費用。

### 3.3 設定費

「客戶」應就「交易文件」所載設定支付費用。

## 4. 期間及續約選項

IBM SaaS 之期間，自 IBM 通知「客戶」其可存取 IBM SaaS 之當日起算，詳如「權利證明書」上所載。「權利證明書」將載明 IBM SaaS 是要自動續約、持續使用方式，或於期間結束時終止。

如係自動續約，除非「客戶」於前項期間到期日三十日（或更早）前為不續約之書面通知，否則，IBM SaaS 將依「權利證明書」所載明之期間自動續約。

如係持續使用，將依按月之方式持續提供 IBM SaaS，至「客戶」提供三十日期前終止之書面通知為止。IBM SaaS 將繼續提供至前述三十日期間到期之當月月底。

## 5. 技術支援

於「訂用期間」及 IBM 通知「客戶」已可存取 IBM SaaS 後，會透過線上討論區提供技術支援，並於客戶產生「依使用付款」計費之期間提供作為標準支援。「客戶」可於 IBM SaaS 內提交支援問題單或開啟會談，以尋求協助。IBM 將提供 IBM Software as a Service Support Handbook（IBM 軟體即服務支援手冊），內含技術支援聯絡資訊及其他資訊與程序。

| 嚴重性 | 嚴重性定義 | 回應時間目標 | 回應時間涵蓋範圍 |
|---|---|---|---|
| 1 | **顯著業務影響/服務停機：**<br>業務重要功能無法運作或重要介面故障。此情況通常適用於正式作業環境，且顯示因無法存取服務而對作業造成重要影響。此狀況需要立即解決方案。 | 1 小時內 | 全年無休 |
| 2 | **顯著業務影響：**<br>服務之服務業務特殊裝置或功能使用嚴重受限，或「客戶」有錯過業務截止日之虞。 | 2 營業小時內 | 週一至週五營業時間內 |
| 3 | **次要業務影響：**<br>顯示服務或功能無法使用，但對作業未造成重要影響。 | 4 營業小時內 | 週一至週五營業時間內 |
| 4 | **些微業務影響：**<br>查詢或非技術要求 | 1 個營業日 | 週一至週五營業時間內 |

### 5.1 存取客戶資料

IBM 得基於診斷服務相關問題及有助於服務對「客戶」應用程式進行掃描之目的，而存取客戶資料。IBM 僅限基於修正瑕疵或提供 IBM 產品或服務支援之目的而存取該資料。

## 6. IBM SaaS 供應項目附加條款

安全掃描有可能無法識別應用程式中之一切安全風險，且其設計目的或預定用途非為需要故障保安防護作業之危險環境，包括但不限於航空器導航、空中交通管制系統、武器系統、維生系統、核能設施，或其他於未能識別安全風險時，有可能致生死亡、人身傷害或財產損害之任何應用。安全掃描之運作，不保證運作不會中斷或全無錯誤。

IBM SaaS 可以用來協助「客戶」符合法律、規章、標準或常規所規範的遵循責任。本「服務」所提供的任何指示、建議用法或指引並不會構成法律、會計或其他專業之建議，「客戶」應謹慎以取得自己的法律諮詢或其他專家諮詢。「客戶」應負責確保「客戶」及「客戶」的活動、應用程式及系統遵守所有適用之法律、規章、標準及常規。「本服務」之使用，不保證遵循一切法律、法規、標準或常規。

IBM SaaS 會對「客戶」選擇掃描之網站及 Web 或行動式應用程式進行侵入性及非侵入性測試。若干法律禁止在未獲授權之情形下嘗試滲透或存取電腦系統。「客戶」授權 IBM 執行本使用條款所定「服務」，並確認此等「服務」包含對「客戶」電腦系統之授權存取。如 IBM 認為執行「服務」有必要時得將前揭授權之授與揭露予第三人者。

本測試伴隨若干風險，包括且不限於下列風險：

a. 「客戶」之電腦系統在測試期間執行應用程式時可能會當機或損毀，因而致使系統暫時無法使用，或造成資料遺失；

b. 於進行測試之期間，「客戶」系統之效能與傳輸量，以及相關路由器與防火牆之效能與傳輸量，可能會發生暫時欠佳之情形；

c. 可能會產生大量日誌訊息，因而造成大量耗用日誌檔磁碟空間之情形；

d. 資料可能會因漏洞探測而被變更或刪除；

e. 侵入偵測系統可能會觸發警示；

f. 受測 Web 應用程式之電子郵件功能可能會引發電子郵件；

g. 本 IBM SaaS 可能基於尋找事件之目的而截取受監視之網路資料流量。

任何由 IBM 提供之服務水準協定權利或補救辦法，以及有關接受測試之網站或應用程式，皆於測試活動進行期間悉予拋棄。

若「客戶」將受測應用程式之已鑑別登入認證輸入本「服務」中，「客戶」應該只輸入測試帳戶（而非正式作業使用者）適用之該等認證。使用正式作業使用者認證，可能會導致透過本「服務」傳輸個人資料之情形。

IBM SaaS 得配置來掃描正式作業 Web 應用程式。當「客戶」設定掃描類型為「正式作業」時，該服務之設計是以減低上列風險的方式執行掃描；但是，在某些情況下，本 IBM SaaS 可能導致所測試之正式作業網站和基礎架構內效能降低或不穩定。在使用本 IBM SaaS 掃描正式作業網站的合適性方面，IBM 不做任何保證或聲明。

「客戶」應自行負責判斷本「服務」對於「客戶」之網站、Web 應用程式、行動式應用程式或技術環境是否適用或安全無虞。

IBM SaaS 之設計目的，在於識別行動式及 Web 應用程式和 Web 服務中各種潛在之安全與法規遵循問題。它無法測試所有漏洞或法規遵循風險，也不具防堵安全攻擊之功能。安全威脅、規章及標準不斷變更，因此，本「服務」可能無法反映此類之一切變更。「客戶」之 Web 應用程式、系統與員工之安全與法規遵循，以及補救行動，均由「客戶」自行負責。使用或不使用本「服務」提供之資訊，由「客戶」自行決定。

若干法律禁止在未獲授權之情形下嘗試滲透或存取電腦系統。「客戶」應負責確保「客戶」不使用本「服務」掃描非「客戶」所擁有或「客戶」不具掃描權限及授權之任何網站及/或應用程式。

為求語意之明確，特別說明如下：「IBM 使用條款 - 一般條款」資料保護一節所載「客戶」內容，亦視同包含 IBM 於執行「應用程式滲透測試」時可能存取之資料。

## 6.1 第三人所有之系統

就第三人所有供測試對象之系統（基於本條款之目的，此系統包括但不限於應用程式及 IP 位址），「客戶」同意：

a. 於 IBM 在第三人系統上開始進行測試之前，「客戶」應向各系統所有人取得業經簽署之授權書，授權 IBM 得於該系統上提供「服務」，且該授權書應載明各該所有人同意標題為「測試執行許可」一節所訂條款，此外，「客戶」應提供 IBM 一份該授權書；

b. 自行負責向系統所有人傳達進行 IBM 遠端測試時於該等系統上識別之任何風險、曝露及漏洞；及

c. 於 IBM 認為有必要時，安排及幫助系統所有人與 IBM 之間資訊交換相關事宜。

「客戶」同意：

- 本測試對象之系統所有人有異動時，應即通知 IBM；
- 非經 IBM 事前書面同意，不得於「客戶企業」外部揭露交付項目或揭露 IBM 曾執行前揭「服務」之事實；及
- 因「客戶」未能遵循標題為「第三人所有之系統」該節之規定所致第三人求償，以及因任何第三人基於下列事由對 IBM 或其承包商或代理商所為之索賠或主張，而致 IBM 蒙受損失或須負賠償責任者，「客戶」應完全賠償 IBM 所受之損害：(a) 測試對象之系統，進行系統之安全風險、曝露或漏洞等項目之測試； (b) 將該測試之結果提供予「客戶」；或 (c)「客戶」對該等結果之使用或揭露。

## 6.2 Cookie

「客戶」知悉並同意，IBM 得就 IBM SaaS 之使用，藉由追蹤及其他技術，蒐集「客戶」（「客戶」之員工及約聘人員）所提供之個人資料，以作為 IBM SaaS 一般作業及支援之一部分。IBM 蒐集前述資料之目的，在於蒐集有關 IBM SaaS 效率之使用統計資料與資訊，以改善使用者之使用體驗及/或調整與「客戶」之互動方式。「客戶」確認其將取得或已取得同意，以允許 IBM 及其承包商執行業務時，得依適用法律，基於前項目的，於 IBM、其他 IBM 公司及其承包商內處理前項所蒐集之個人資料。IBM 將依「客戶」之員工及約聘人員之要求，存取、更新、更正或刪除其所蒐集之個人資料。

作為 IBM SaaS 之一部分（包括報告活動），IBM 將編製及維護從 IBM SaaS 蒐集之去識別化及/或聚集資訊（稱為「安全資料」）。「安全資料」不識別「客戶」或個人，但以下第 (d) 款另有規定者不在此限。「客戶」在此同意 IBM 僅限基於下列目的而使用及/或複製「安全資料」：

a. 發佈及/或散布「安全資料」（例如：在進行有關網路安全之編譯及/或分析時）。

b. 開發或加強產品或服務；

c. 在內部進行研究，或與第三人進行研究；及

d. 合法分享業經確認之第三人犯罪資訊。

## 6.3 衍生受益之地點

在適用情形下，稅金之核算係以「客戶」於其收受 IBM SaaS 之權益時所指明地點為依據。除非「客戶」提供其他資訊予 IBM，否則 IBM 於核算稅金時，將以下列公司地址為依據，該地址係「客戶」訂購 IBM SaaS 時指明為主要受益地點。「客戶」應負責保持最新之前述資訊，並將其變更提供予 IBM。

## 6.4 個人資料與受管理內容及服務

本 IBM SaaS 並非專為受管理內容之特定安全需求而設計，例如：個人資料或機密個人資料。「客戶」應自行負責判斷，就「客戶」搭配 IBM SaaS 一併使用之內容類型而言，本 IBM SaaS 是否符合「客戶」之需求。

IBM 非以美國聯邦通信委員會 ("FCC") 或州立主管機關（「州立主管機關」）規定之服務提供者身分運作，亦無意提供任何受 FCC 或「州立主管機關」管轄之服務。倘 FCC 或「州立主管機關」就 IBM 依本使用條款提供之服務訂有相關法規或義務，IBM 得為下列行為：(a) 修改、更換或替換產品，所需費用由「客戶」支付；及/或 (b) 變更提供前揭服務之方式，使 IBM 免受該等法規或義務之拘束（例如：以「客戶」代理人之身分，從第三人公用事業者取得前揭服務）。

# 附錄 A

## 1. IBM Application Security on Cloud 一般說明

IBM Application Security on Cloud 提供單一位置，協助「客戶」識別各種應用程式之安全漏洞（例如：「SQL 資料隱碼攻擊」、「跨網站 Scripting」及「資料洩漏」）。本服務包含各種類型之應用程式安全掃描技術，可個別用以指明該應用程式中之安全問題。

IBM Application Security on Cloud 提供下列功能：

- 掃描行動式應用程式，以確認有無安全漏洞。此項掃描作業係透過動態 (blackbox) 及互動式 (glassbox) 安全分析技術執行。
- 掃描正式作業或前置正式作業網站、公開或專用網路上之網站，以確認有無安全漏洞。此項掃描作業係透過動態 (blackbox) 安全分析技術執行。
- 掃描 Web 應用程式及桌上型電腦應用程式內之資料流程，以確認有無安全漏洞。此項掃描作業係透過靜態 (whitebox) 安全分析技術執行。
- 提供詳細之安全漏洞報告，載明發現項目之高階摘要及可供開發人員遵循之補救步驟。
- 與各種 DevOps 平台整合

### 1.1 IBM Application Analyzer

IBM Application Analyzer 得依「應用程式實例」、「工作」（掃描）或以完整「實例」訂購之，且允許進行下列掃描類型：

- Dynamic Analyzer - 透過 DAST 技術進行前置正式作業或正式作業網站測試
- Mobile Analyzer - 透過 IAST 技術進行 iOS 或 Android 二進位檔測試
- Static Analyzer - 透過 SAST 技術測試位元組或原始碼資料流程

### 1.2 設定服務

IBM Application Security on Cloud Consulting Services 是 Application Analyzer 之產品化設定服務。本「服務」含 IBM 顧問提供有關應用程式風險測試與管理之指導與協助。IBM Application Security on Cloud Consulting Services 係以「約定」區塊之方式購買，該等區塊可於以下所定數量中展開，以要求及使用下列特定服務：

a. **Fast Start** [使用一 (1) 個「約定」單位]

Fast Start 服務提供有關使用 Application Security on Cloud 測試及風險管理特性之專門知識及指引。於「客戶」確認已成功登入 Application Security on Cloud 入口網站後，IBM 會協助召開上限為二 (2) 小時之網路會議並提供二 (2) 位線上參與者，以提供有關基本 AppSec on IBM SaaS 配置與功能之教育訓練，包括掃描類型、執行掃描、審查報告及安裝相關工具及外掛程式。Fast Start 服務將於下列項目完成後即為完成：(a) 客戶教育訓練網路研討會；(b) 適用工具及外掛程式之安裝；及 (c) 協助「客戶」設定及執行「客戶」之首次掃描。

b. **Assessment Review** [使用二 (2) 個「約定」單位]

本 Assessment Review 服務可協助審查測試結果，包括瞭解應用程式漏洞修正並設定該項修正之優先順序。IBM 將協助召開上限為一 (1) 小時之網路會議並提供二 (2) 位線上參與者，以提供所發現漏洞之概觀與整體應用程式安全風險，以及所發現應用程式安全漏洞之詳細討論，包括 (1) 漏洞測試方式；(2) 漏洞偵測方式； (3) 各項漏洞之風險；及 (4) 提供一般修正建議，協助修正漏洞。前項審查係完全以測試結果為依據，且非為原始碼本身之審查。「客戶」於網路會議開始進行之前，應先審查測試結果，並向 IBM 確認所要審查之測試結果。本 Assessment Review 服務將於網路會議完畢即為完成。

c. **Scan for Me** [使用四 (4) 個「約定」單位]

本 Scan for Me 服務提供一位 IBM 應用程式安全專家，由該專家負責配置及執行掃描、驗證結果及進行審查發現項目之簡報。「客戶」應允許 IBM 顧問進出其 ASoC 環境，以配置及執行掃描、驗證結果及提供有關修正優先順序之建議，並進行結果簡報。IBM 將協助召開上限為一 (1) 小時之網路會議並提供二 (2) 位線上參與者，以提供所發現漏洞之概觀與整體應用程式安全風險，以及所發現應用程式安全漏洞之詳細討論，包括 (1) 漏洞測試方式；(2) 漏洞偵測方式； (3) 各項漏洞之風險；及 (4) 提供一般修正建議，協助修正漏洞。業經提出，且於首次掃描後達 30 日者，IBM 僅限使用原始掃描配置進行重新掃描以驗證安全修正程式，不得測試新功能、驗證結果及交付報告予客戶。本 Scan for Me 服務將於審查首次掃描結果之網路會議完畢時即為完成，或在適用情形下，於完成「客戶」所要求執行之重新掃描及交付重新掃描報告予「客戶」時即為完成。

d. **Advisor on Demand** [使用七 (7) 個「約定」單位]

本 Advisor on Demand 服務提供至多上限為二十 (20) 小時 IBM 顧問時間，該時間可用於進行有關本 IBM SaaS 之各項活動。前揭 IBM 顧問將協助處理應用程式安全特定主題，包括但不限於程式管理、安全測試優先順序、修正策略、原始碼分析及原始碼修復。IBM 將協同「客戶」瞭解及建立包含特定「客戶」需求之專案時程，包括專案目標、相關技術、所要時間表、預期交付項目，以及 Advisor on Demand 服務約定預估數量等需求。「客戶」必須提供於執行服務時所需之必要應用程式、系統及說明文件之存取權限。本 Advisor on Demand 服務，於安全專門技術之施行已達 上限 20 小時，及/或於專案時程及/或於專案時程所載交付項目已交付「客戶」後，即為完成。

e. **Application Penetration Testing**

三個選項：

(1) **循規準則/入門應用程式滲透測試** - 包括最多上限四十 (40) 小時「顧問」時間，並以單步驟邏輯缺失及簡易版資料隱碼攻擊缺失為其重點。使用十五 (15) 個「約定」單位。

(2) **標準應用程式滲透測試** - 包括最多上限六十 (60) 小時「顧問」時間，並擴充其重點，以包含多步驟工作流程中之邏輯缺失、複式版資料隱碼攻擊缺失及複式資料類型分析。使用二十一 (21) 個「約定」單位。

(3) **進階應用程式滲透測試** - 最多上限八十 (80) 小時「顧問」時間，並擴充其重點，以包含已編譯執行檔、客製網路通訊協定之剖析、公開使用之檔案庫及架構之深度分析。使用二十七 (27) 個「約定」單位。

本應用程式滲透測試服務所提供之 IBM 資源，可用於執行應用程式之測試及不當運用、測試報告之交付及用以說明發現項目及相關風險之簡報。

IBM 將協助召開上限為一 (1) 小時之專案起始會議並提供二 (2) 位線上參與者，以審查「客戶」之環境及組織，包括應用程式平台、結構、架構、支援基礎架構、應用程式相關已知安全問題或考量、初步測試時程及緊急聯絡計劃。

IBM 將執行應用程式滲透測試，包括但不限於以下各項：識別一般漏洞（例如：SQL 資料隱碼攻擊）、評量現有安全管控項目之優缺點（例如：輸入驗證、鑑別及授權等項目）、檢查是否適當施行商業邏輯、驗證是否適當使用安全通訊協定、識別階段作業處理缺失，以及驗證是否針對登入、密碼回復、密碼原則及其他使用者管理功能設定適當之安全管控項目。發現項目將記載於「應用程式滲透測試報告」中。IBM 將協助召開網路會議，並於該會議中進行上限為一 (1) 小時之簡報。本 Application Penetration Test 服務，於獲配諮詢時間用盡、網路會議完畢及最終「應用程式滲透測試報告」已交付「客戶」時，即為完成。

### 1.2.1 設定服務之責任

IBM 將：

- 依「權利證明書」之規定，使用「客戶」所購買之「約定」單位提供「設定服務」；及
- 於達成第 1.2 節所載完工標準時已完成「設定服務」。

「客戶」同意：

- 應負責支付有關「客戶」於契約期間所為一切「約定」要求之一切費用。
- 並承認所購買之「約定」單位應於起始契約期間內使用，未於該契約期間結束日期前用畢者，視同到期；及
- 應於訂用結束日期前至少 30 日，開始提出一切「設定服務」之正式要求。

於執行「設定服務」時，IBM 得向「客戶」索取資訊及要求合理之配合。「客戶」未能及時就所索取之資訊或所要求予以配合者，可能致生由 IBM 訂定之服務所需「約定」單位費用，或致使適用服務之延遲執行。

為使 IBM 得以準確執行測試，「客戶」同意遵循 IBM 就測試期間環境之準備與維護所給予之指示。