

## 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/>。

如互有抵觸者, 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

### 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. 「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, 故各需備有一份授權。「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, 取得足夠涵蓋連接至 IBM SaaS 之「應用程式實例」數量之授權數。

### 3. 計費及付款

IBM SaaS 的付款金額明訂於「交易文件」中。

#### 3.1 依使用付款

「依使用付款」選項之發票將於使用服務後之該月, 依「交易文件」規定之費率開立。

#### 3.2 部分每月費用

「交易文件」所定部分每月費用得按比例計算之。

### 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」之規定。權利證明書應載明 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」於前項期間到期日九十日 (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 90 日期前終止之書面通知為止。IBM SaaS 將繼續提供至前述九十日期間到期之日當月底。

### 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	<b>顯著業務影響/服務停機：</b> 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	<b>顯著業務影響：</b> 所服務之業務特殊裝置或功能使用受限，或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	<b>次要業務影響：</b> 表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	<b>些微業務影響：</b> 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

安全掃描未必能識別應用程式中的所有安全風險。

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，此等測試伴隨若干風險，包括且不限於下列風險：

- 「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；
- 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；
- 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；
- 資料可能會因漏洞探測而被變更或刪除；
- 侵入偵測系統可能會觸發警示；
- 受測 Web 應用程式之電子郵件功能可能會引發電子郵件；
- 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。

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。

## 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 一般運作及支援之一部分。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。

## 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。

## 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、公開或私密網路上之網站，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（例如：Maven 及 IBM UrbanCode）整合。