IBM Security Trusteer Fraud Protection

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）（合稱為「合約」）之規範，「合約」與「使用條款」共同構成本完整合約。

1. IBM SaaS

前項 SaaS 特定供應項目條款涵蓋而適用於下列 IBM SaaS 供應項目：

1.1 Rapport IBM SaaS 供應項目

- IBM Security Trusteer Rapport for Business
- IBM Security Trusteer Rapport for Business Premium Support
- IBM Security Trusteer Rapport for Retail
- IBM Security Trusteer Rapport for Retail Premium Support
- IBM Security Trusteer Rapport Fraud Feeds for Business
- IBM Security Trusteer Rapport Fraud Feeds for Business Premium Support
- IBM Security Trusteer Rapport Fraud Feeds for Retail
- IBM Security Trusteer Rapport Fraud Feeds for Retail Premium Support
- IBM Security Trusteer Rapport Phishing Protection for Business
- IBM Security Trusteer Rapport Phishing Protection for Business Premium Support
- IBM Security Trusteer Rapport Phishing Protection for Retail
- IBM Security Trusteer Rapport Phishing Protection for Retail Premium Support
- IBM Security Trusteer Rapport Mandatory Service for Business
- IBM Security Trusteer Rapport Mandatory Service for Retail

1.2 Pinpoint IBM SaaS 供應項目

- IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition
- IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition Premium Support
- IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition
- IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition Premium Support
- IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition
- IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition Premium Support
- IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition
- IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition Premium Support
- IBM Security Trusteer Pinpoint Criminal Detection for Business
- IBM Security Trusteer Pinpoint Criminal Detection for Business Premium Support
- IBM Security Trusteer Pinpoint Criminal Detection for Retail
- IBM Security Trusteer Pinpoint Criminal Detection for Retail Premium Support
- IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile
- IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile Premium Support

- IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile
- IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile Premium Support
- IBM Security Trusteer Pinpoint Carbon Copy for Business
- IBM Security Trusteer Pinpoint Carbon Copy for Business Premium Support
- IBM Security Trusteer Pinpoint Carbon Copy for Retail
- IBM Security Trusteer Pinpoint Carbon Copy for Retail Premium Support
- IBM Security Trusteer Rapport Remediation for Retail
- IBM Security Trusteer Rapport Remediation for Retail Premium Support

1.3 行動式 IBM SaaS 供應項目

- IBM Security Trusteer Mobile SDK for Business
- IBM Security Trusteer Mobile SDK for Retail
- IBM Security Trusteer Mobile Browser for Business
- IBM Security Trusteer Mobile Browser for Business Premium Support
- IBM Security Trusteer Mobile Browser for Retail
- IBM Security Trusteer Mobile Browser for Retail Premium Support

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. **「合格參與者」**- 是取得 IBM SaaS 所依據的一種計量單位。「個人」或「實體」是取得由 IBM SaaS 管理或追蹤之任何服務遞送程式之參與資格者，即為「合格參與者」。「客戶」應在其「交易文件」中所指定的計量期間，取得足夠涵蓋於 IBM SaaS 內管理或追蹤之所有「合格參與者」的授權數。

由 IBM SaaS 管理之每一項服務交付程式，均先予以個別分析後再合併。符合多重服務遞送程式資格之個人或實體，需取得個別授權。

就前項供應項目，服務交付程式包含「客戶」之單一「商業應用程式」或「零售業應用程式」，各「商業應用程式」或「零售業應用程式」均有其主要登入頁面及相關頁面。「合格參與者」係指「客戶」之「終端使用者」，該使用者備有「商業應用程式」或「零售業應用程式」之登入認證。

b. **「用戶端裝置」**- 是取得 IBM SaaS 所依據的一種計量單位。「用戶端裝置」係指一種單一使用者運算裝置或具特殊用途之感應器或遙測裝置，該裝置要求執行來自另一電腦系統（通常稱為伺服器或由伺服器管理）之一組指令、程序或應用程式，或接受該組指令、程序或應用程式之執行結果，或提供資訊予該系統。多個用戶端裝置可使用同一部共用伺服器。用戶端裝置可能具備某些處理能力，亦可能為可程式化，容許使用者執行工作。在「客戶」的「交易文件」中所指定的計量期間，「客戶」應為執行 IBM SaaS、提供資料給 IBM SaaS、使用由 IBM SaaS 提供的服務，或以其他方式存取 IBM SaaS 之每一個「用戶端裝置」取得授權。

3. 計費及付款

IBM SaaS 的付款金額明訂於「交易文件」中。

3.1 局部月計費

「交易文件」所定局部月計費得按比例評定之。

4. 遵循授權規定及查核

對 IBM Security Trusteer Fraud Protection 供應項目之存取，受「交易文件」中指定之「合格參與者」或「用戶端裝置」最高數量之規範。「客戶」應負責確認其「合格參與者」或「用戶端裝置」之數量，未超過「交易文件」中規定之「合格參與者」或「用戶端裝置」之上限數量。

IBM 得不定時執行查核以確認是否遵循所規定之「合格參與者」或「用戶端裝置」之最高數量限制。

5. IBM SaaS 訂用期間續約選項

「客戶」之「交易文件」應依下列其中一種方式指定「訂用期間」，以明訂 IBM SaaS 是否於「訂用期間」終止時續約：

5.1 自動續約

若「客戶」之「交易文件」載明「客戶」採自動續約之方式，「客戶」得於「交易文件」所載期間到期日至少九十日前，以書面要求「客戶」之 IBM 業務代表或 IBM 事業夥伴終止即將到期之「IBM SaaS 訂用期間」。若 IBM 或其 IBM 事業夥伴於到期日前未收到前項終止通知，前項即將到期之「訂用期間」將自動續約一年，或視為續約與「交易文件」所訂原始「訂用期間」相同之期間。

5.2 持續計費

若「交易文件」載明「客戶」係採持續之續約方式，則「客戶」得繼續存取 IBM SaaS，並依持續之續約方式，就 IBM SaaS 之使用情形予以計費。若要中斷使用 IBM SaaS 並停止持續計費程序，「客戶」應於九十 (90) 日前以書面向 IBM 或其 IBM 事業夥伴通知，要求終止其 IBM SaaS。 於「客戶」終止存取權時，「客戶」應支付之費用包含到終止生效之該月為止之任何尚未結清之存取費用。

5.3 必須之續約

若「交易文件」載明「客戶」之續約類型為「終止」者，則將於「訂用期間」結束時終止 IBM SaaS ，並移除「客戶」對 IBM SaaS 之存取權。若要在前項終止日後繼續使用 IBM SaaS，「客戶」應向「客戶」之 IBM 業務代表或 IBM 事業夥伴下訂單，以購買新「訂用期間」。

6. 技術支援

IBM 將為「客戶」及其「合格參與者」提供 IBM SaaS 技術支援，以協助其使用 IBM SaaS。

一切供應項目之訂用，均包含「標準支援」。Trusteer Rapport Mandatory Service 係 Trusteer Rapport 之附加程式，此程式係訂用基本程式 Trusteer Rapport 之頂級支援所須具備之必要條件。

提供每一 IBM SaaS 供應項目之頂級支援，須另外收取費用，但 IBM Security Trusteer Mobile SDK 供應項目及 IBM Security Trusteer Rapport Mandatory Service 供應項目除外。

標準支援：

- 於當地時間早上 8 點至下午 5 點提供支援。
- 「客戶」及其「合格參與者」可採電子方式提交支援問題單，相關資訊詳述於《軟體即服務 [SaaS] 支援手冊》。
- 「客戶」可造訪「用戶端支援入口網站」，以瞭解通知、文件、案例報告及常見問題 (FAQ) 相關資訊（網址：http://www-01.ibm.com/software/security/trusteer/support/）。
- 有關支援選項與詳細資料，請存取 IBM Software as a Service [SaaS] Support Handbook（IBM 軟體即服務支援手冊），網址如下：http://www-01.ibm.com/software/support/handbook.html。

頂級支援：

- 為所有嚴重性的問題提供全年無休支援。
- 「客戶」可直接透過電話取得支援。
- 「客戶」及其「合格參與者」可採電子方式提交支援問題單，相關資訊詳述於《軟體即服務 [SaaS] 支援手冊》。
- 「客戶」可造訪「用戶端支援入口網站」，以瞭解通知、文件、案例報告及常見問題 (FAQ) 相關資訊（網址：http://www-01.ibm.com/software/security/trusteer/support/）。
- 有關支援選項與詳細資料，請存取 IBM Software as a Service [SaaS] Support Handbook（IBM 軟體即服務支援手冊），網址如下：http://www-01.ibm.com/software/support/handbook.html。

7. IBM SaaS 供應項目附加條款

7.1 安全港法規遵循

IBM 遵循「美國商務部」協同歐洲聯盟委員會一併研發之「美國與歐盟安全港架構」。IBM Security Trusteer 產品包含於 IBM 之「歐盟與美國安全港」認證。有關「安全港」之其他資訊及「安全港」公司清單，均可在下列網站找到：http://export.gov/safeharbor/。

7.2 客戶年訂用費之調增

IBM 保留依相當百分比調整 IBM SaaS 訂用費之權利，每十二 (12) 個月至多調整一次，訂用費調整百分比由 IBM 決定，但以 3% 為其上限。訂用費調整將於最初涵蓋期間之週年起始日生效。此費用之調整不會變更「客戶」之 IBM SaaS 授權，也不會變更已取得 IBM SaaS 時所依據之計費度量。本公司之事業夥伴與本公司係各自獨立之法人，其得自行訂定其價格及條款並不受本公司拘束。

7.3 頂級支援

「客戶」僅獲授權對「客戶」已訂用相關「頂級支援」供應項目之 IBM SaaS 供應項目享有「頂級支援」。

7.4 合法使用與同意

蒐集及處理資料之授權

IBM SaaS 之設計，旨在協助「客戶」改善其安全環境及資料。就「客戶」訂用 IBM SaaS 供應項目所涵蓋之「商業應用程式」或「零售業應用程式」項目後，IBM SaaS 將蒐集與該應用程式互動之「合格參與者」及「用戶端裝置」所提供之資料。在某些管轄權區域，IBM SaaS 所蒐集資料之本身或其組合可能被視為「個人資料」。「個人資料」係指任何可以用來識別特定個人的資訊（例如，姓名、電子郵件位址、住家地址或電話號碼），可以提供給 IBM 以代表「客戶」進行儲存、處理或傳輸。

為改進 IBM SaaS 之功能，可能會更新資料之蒐集與處理規定。必要時，也會更新資料蒐集與處理規定完整說明之文件，並於「客戶」提出要求時為其提供該文件。「客戶」授權 IBM 依本使用條款之「跨境傳輸」一節及「資料隱私權」一節，以及使用條款一般條款之「資料隱私權與資料安全」一節之規定，蒐集及處理前項資料。

下列規定適用於 IBM Security Trusteer Pinpoint 供應項目：

所蒐集之資料可能包括使用者 IP 位址、已加密或單向雜湊使用者 ID、網域 Cookie（若未過濾）、造訪受保護「應用程式」及網路釣魚網站、地理位置之記錄，以及進入網路釣魚網站之認證。

下列規定適用於 IBM Security Trusteer Mobile SDK 供應項目及 IBM Security Trusteer Mobile Browser 供應項目：

所蒐集之資料可能包括使用者 IP 位址、已加密或單向雜湊使用者 ID、地理位置，以及造訪受保護「應用程式」、SIM 卡資訊、裝置名稱及客戶連結之記錄。

下列規定適用於 IBM Security Trusteer Rapport 供應項目：

所蒐集之資料可能包括使用者 IP 位址、已加密或單向雜湊使用者 ID、安全事件、為聯絡 IBM 以要求「客戶」支援而提供之使用者名稱及電子郵件位址、客戶連結、進入受保護網站時所輸入之已加密密碼、造訪受保護「應用程式」及網路釣魚網站之記錄、已加密之付款卡號，以及 IBM 人員為偵測可疑惡意軟體、惡意活動或故障而從遠端蒐集之檔案及資料。

資料當事人之告知後同意：

本 IBM SaaS 之使用可能涉及各種法令規章之適用，IBM SaaS 僅限基於合法之目的且以合法方式使用之。「客戶」同意依適用法令規章及政策之規定使用 IBM SaaS，並對遵循該等法令規章及政策負完全之責。

下列規定適用於 IBM Security Trusteer Pinpoint 供應項目及 IBM Security Trusteer Mobile SDK 供應項目：

「客戶」同意其已取得或將取得具充分告知後之必要同意、許可或授權，得合法使用 IBM SaaS 及允許 IBM 透過 IBM SaaS 蒐集及處理資訊。

下列規定適用於 IBM Security Trusteer Rapport 供應項目及 IBM Security Trusteer Mobile Browser 供應項目：

「客戶」授權 IBM 取得具充分告知後之必要同意，得合法使用 IBM SaaS 及蒐集與處理「終端使用者授權合約」，可參照下列網址 https://www.trusteer.com/support/end-user-license-agreement 所示資訊。若「客戶」決定由其本身（而非 IBM）處理為取得終端使用者之同意所為通訊之相關事宜，「客戶」同意其已取得或將取得具充分告知後之必要同意、許可或授權，得合法使用 IBM SaaS 及允許 IBM（作為「客戶」之資料處理者）透過 IBM SaaS 蒐集及處理資訊。

7.5 跨境傳輸

「客戶」同意 IBM 得依相關法律與規定，在「歐洲經濟區」境外下列國家及「歐盟執行委員會」認為具備適當安全等級之國家以身為處理者及再處理者，而跨境處理內容（包括「個人資料」）：美國。

7.6 資料保密

如「客戶」係於歐盟成員國、冰島、列支敦斯登、挪威或瑞士將「個人資料」提供給 IBM SaaS，或「客戶」在該等國家中有「合格參與者」或「用戶端裝置」，則「客戶」（作為唯一控制者 (controller)）得指定 IBM（作為處理者 (processor)）處理「個人資料」（該等名詞定義收錄於 EU Directive 95/46/EC）。IBM 僅限依其所發佈之 IBM SaaS 說明，基於提供 IBM SaaS 供應項目之必要而處理前述「個人資料」，且「客戶」同意該項處理係依「客戶」之指示為之。IBM 對於前項處理位置或其保護屬於 IBM SaaS 一部分之「個人資料」之方式如有重大變更，應於事前為合理之通知。「客戶」得於 IBM 將此變更通知「客戶」後的三十 (30) 日內，以書面通知 IBM 終止受影響 IBM SaaS 的現行「訂用期間」。「客戶」同意 IBM 得以處理者及再處理者而跨境處理下列「內容」（包括「個人資料」）：

處理者/再處理者名稱	角色（資料處理者或再處理者）	位置*
IBM 締約實體	處理者	如交易文件所定
Amazon Web Services LLC	再處理者	410 Terry Ave. N Seattle, WA 98109 台灣
Connectria Corp.	再處理者	10845 Olive Blvd., Suite 300 St. Louis, MO 63141 台灣
IBM Israel Ltd.	再處理者	94 Derech Em-Hamoshavot 49527 Petach-Tikva 以色列
IBM Corp	再處理者	1 New Orchard Rd. Armonk, NY 10504 台灣

「客戶」同意 IBM 於其認為有合理必要提供 IBM SaaS 時，得變更前項國家或地區位置之清單。

「客戶」同意，就於提供程序進行期間所定，透過德國資料中心所提供之服務，IBM 得以處理者及再處理者而跨境處理下列內容（包括「個人資料」）：

處理者/再處理者名稱	角色（資料處理者或再處理者）	位置*
IBM 締約實體	處理者	如交易文件所定
Amazon Web Services（德國）	再處理者	德國慕尼黑
IBM Israel Ltd.	再處理者	94 Derech Em-Hamoshavot 49527 Petach-Tikva 以色列

「客戶」同意，就於提供程序進行期間所定，透過日本資料中心所提供之服務，IBM 得以處理者及再處理者而跨境處理下列內容（包括「個人資料」）：

處理者/再處理者名稱	角色（資料處理者或再處理者）	位置*
IBM 締約實體	處理者	如交易文件所定
Amazon Web Services（日本）	再處理者	日本東京
IBM Israel Ltd.	再處理者	94 Derech Em-Hamoshavot 49527 Petach-Tikva 以色列

* 上表載明之位置包括處理者/再處理者公司的辦公室地址。資料中心位於載明之相同國家。

雙方當事人或其關係企業得依已移除選用條款之「EC 決策 2010/87/歐盟」，按其對應之角色簽訂個別標準未修改之「歐盟模型條款」合約。前述合約，縱使係由關係企業所簽訂，其所生一切爭議或責任，仍視為本「合約」之條款所生雙方當事人間的爭議或責任。

附錄 A

1. IBM SaaS 供應項目

IBM 供應前揭服務作為獨立式服務與供應項目，或額外服務與供應項目。所訂購之特定 IBM SaaS 供應項目載明於「客戶」之權利證明書。

1.1 商業與零售業定義

須搭配使用特定「應用程式」類型，方能取得 IBM Security Trusteer 防詐欺產品之授權。所稱「應用程式」係定義為下列其中一種類型：「零售業」或「商業」。「零售業應用程式」及「商業應用程式」各有其不同適用之供應項目。

- 所稱「零售業應用程式」，係指專為提供客戶各項服務而設計之線上銀行業應用系統、行動式應用程式或電子商務應用程式。「客戶」政策可將某些小型業務分類成適用於零售業存取。
- 所稱「商業應用程式」，係指專為提供各項服務予公司、機關或同等實體而設計之線上銀行業應用系統、行動式應用程式或電子商務應用程式，或其他未被分類為「零售業」之應用程式。

1.2 IBM SaaS Base Subscription 供應項目

商業供應項目：

- IBM Security Trusteer Rapport for Business
- IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition
- IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition
- IBM Security Trusteer Pinpoint Criminal Detection for Business
- IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile
- IBM Security Trusteer Mobile SDK for Business
- IBM Security Trusteer Mobile Browser for Business

零售業供應項目：

- IBM Security Trusteer Rapport for Retail
- IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition
- IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition
- IBM Security Trusteer Pinpoint Criminal Detection for Retail
- IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile
- IBM Security Trusteer Mobile SDK for Retail
- IBM Security Trusteer Mobile Browser for Retail

每一種「商業」供應項目及「零售業」供應項目各有其相關「頂級支援」產品，該等產品之提供，須另外收取費用，但 IBM Security Trusteer Mobile SDK 供應項目除外。

1.3 IBM Security Trusteer Rapport 供應項目適用之額外 IBM SaaS Subscription 供應項目

IBM Security Trusteer Rapport for Business 適用之額外供應項目：

- IBM Security Trusteer Rapport Fraud Feeds for Business
- IBM Security Trusteer Rapport Phishing Protection for Business
- IBM Security Trusteer Rapport Mandatory Service for Business

IBM Security Trusteer Rapport for Retail 適用之額外供應項目：

- IBM Security Trusteer Rapport Fraud Feeds for Retail
- IBM Security Trusteer Rapport Phishing Protection for Retail
- IBM Security Trusteer Rapport Mandatory Service for Retail

每一種 IBM Security Trusteer Rapport 供應項目之「商業」及「零售業」附加程式各有其相關「頂級支援」產品，該等產品之提供須另外收取費用，但 IBM Security Trusteer Rapport Mandatory Service 附加程式除外。

IBM Security Trusteer Rapport for Business 或 IBM Security Trusteer Rapport for Retail 之訂用係為本節所列相關額外 IBM SaaS 訂用供應項目之必備項目。

1.4 IBM Security Trusteer Pinpoint Malware Detection 供應項目適用之額外 IBM SaaS Subscription 供應項目

IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition 或 IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition 適用之額外供應項目：

- IBM Security Trusteer Pinpoint Carbon Copy for Business

IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition 或 IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition 適用之額外供應項目：

- IBM Security Trusteer Pinpoint Carbon Copy for Retail
- IBM Security Trusteer Rapport Remediation for Retail

本節所列每一額外 IBM SaaS 供應項目各有其適用之「頂級支援」訂用，此訂用須另外收取費用。

IBM Security Trusteer Pinpoint Malware Detection for Business 供應項目或 IBM Security Trusteer Pinpoint Malware Detection for Retail 供應項目之訂用，係為本節所列相關額外 IBM SaaS 訂用供應項目之必備項目。

1.5 其他額外 IBM SaaS 訂用

此處未列出前揭基本程式訂用所適用之額外 IBM SaaS Subscription，無論目前已提供或正在開發都不被視為更新項目，故應另外取得其授權。

1.6 定義

「帳戶持有人」係指「客戶」之「終端使用者」，該使用者已安裝用戶端啟用軟體、已接受終端使用者授權合約 ("EULA")，且至少使用「客戶」之「零售業或商業應用程式」（「客戶」已為該應用程式訂用 IBM SaaS 供應項目涵蓋項目）進行一次鑑別。

「帳戶持有人用戶端軟體」係指 IBM Security Trusteer Rapport 用戶端啟用軟體或 IBM Security Trusteer Mobile Browser 用戶端啟用軟體，以及其他為安裝於終端使用者裝置而隨附於若干 IBM SaaS 訂用之任何用戶端啟用軟體。

"Trusteer Splash" 係指依據可用啟動畫面範本而提供予「客戶」之啟動畫面。

「登入頁面」係指由 IBM 管理之網頁，該網頁可為「客戶」提供「客戶」啟動畫面及可下載之「帳戶持有人用戶端軟體」。

2. IBM Security Trusteer Rapport 供應項目

2.1 IBM Security Trusteer Rapport for Retail 及/或 IBM Security Trusteer Rapport for Business ("Trusteer Rapport")

Trusteer Rapport 提供保護層，以防範網路釣魚及「瀏覽器中間人」(Man-in-the-Browser, MitB) 惡意軟體之攻擊。IBM Security Trusteer Rapport 利用全球數以千萬計的端點所構成之網路，蒐集有關正在對全球各組織進行之網路釣魚及惡意軟體攻擊之情報。IBM Security Trusteer Rapport 採用行為模式演算法，此演算法係以封鎖網路釣魚攻擊及防止 MitB 變形惡意軟體進行安裝及運作為其目標。

本 IBM SaaS 供應項目具有「合格參與者」計費度量。本「商業」供應項目係以 10 位「合格參與者」為一套組之方式銷售。本「零售業」供應項目係以 100 位「合格參與者」為一套組之方式銷售。

本 IBM SaaS 供應項目包括：

a. Trusteer 管理應用程式 ("TMA")：

   TMA 係於 IBM Security Trusteer 雲端管理之環境中提供，透過此應用程式，「客戶」（及其不限數量之授權人員）可執行下列作業：(i) 接收事件資料報告及風險評量；(ii) 檢視、配置及設定有關事件資料報告之政策；及 (iii) 檢視用戶端啟用軟體之配置，此軟體之授權係依終端使用者授權合約

("EULA") 免費提供予大眾，並可供下載至「合格參與者」之桌面或裝置（PC/MAC)，此軟體又稱為 Trusteer Rapport 軟體套件（「帳戶持有人用戶端軟體」）。「客戶」僅限使用 Trusteer Splash 或 Rapport API 行銷「帳戶持有人用戶端軟體」，「客戶」不得將「帳戶持有人用戶端軟體」使用於其內部業務運作或其員工之使用（而非員工之個人使用）。

b. Web Script：

用於為存取或使用 IBM SaaS 供應項目而存取網站。

c. 事件資料：

「客戶」為其「商業應用程式」或「零售業應用程式」訂用 IBM SaaS 供應項目所涵蓋項目後，當「帳戶持有人」與該應用程式進行線上互動時，「帳戶持有人用戶端軟體」便會產生事件資料，此時，「客戶」（及其不限數量之授權人員）可使用 TMA 接收該等事件資料。當「合格參與者」接受 EULA 且至少使用「客戶」之「商業應用程式」或「零售業應用程式」進行一次鑑別後，於該等「合格參與者」之裝置上執行之「帳戶持有人用戶端軟體」所產生之事件資料便會被接收，因此，「客戶」之配置必須包括「使用者 ID」之蒐集。

d. Trusteer Splash：

「客戶」為其「商業應用程式」及/或「零售業應用程式」訂用 IBM SaaS 供應項目所涵蓋項目後，Trusteer Splash 行銷平台便可對存取該等應用程式之「合格參與者」指明及行銷「帳戶持有人用戶端軟體」。「客戶」得從可用的「啟動畫面範本」選取其所要範本。客製啟動畫面得依個別簽立之合約或工作說明書提供之。

「客戶」同意得於搭配使用 TMA 時提供「客戶」之商標、標誌或圖示，惟僅限與 Trusteer Splash 搭配使用，且僅限顯示於「帳戶持有人用戶端軟體」或 IBM 所管理之登入頁面，以及 IBM Security Trusteer 網站。使用「客戶」所提供之商標、標誌或圖示時，應遵循 IBM 就廣告及商標用法所訂定之合理政策。

若「客戶」要使用「帳戶持有人用戶端軟體」之任何必要部署類型，則「客戶」應訂用 IBM Security Trusteer Rapport Mandatory Service SaaS 供應項目。

「帳戶持有人用戶端軟體」之必要部署包括但不限於藉由下列方式進行之必要部署類型：藉由任何機制或方法，直接或間接促使「合格參與者」下載「帳戶持有人用戶端軟體」或藉由建立非由 IBM 建立或核准之任何方法、程序、合約或機制，以略過此「帳戶持有人用戶端軟體」必要部署之授權要件。

2.2 IBM Security Trusteer Rapport for Business 及/或 IBM Security Trusteer Rapport for Retail 適用之選用額外 IBM SaaS 供應項目

IBM Security Trusteer Rapport 供應項目之訂用，係為訂用下列額外 IBM SaaS 供應項目之必要條件。若該 IBM SaaS 載明為「商業適用」，則所取得之額外 IBM SaaS 供應項目亦需載明為「商業適用」。若該 IBM SaaS 載明為「零售業適用」，則所取得之額外 IBM SaaS 供應項目亦需載明為「零售業適用」。當執行「帳戶持有人用戶端軟體」之「合格參與者」接受 EULA 且至少使用「客戶」之「商業應用程式」及/或「零售業應用程式」進行一次鑑別後，該等「合格參與者」所產生之事件資料便會由「客戶」接收，因此，「客戶」之配置必須包括「使用者 ID」之蒐集。

2.2.1 IBM Security Trusteer Rapport Fraud Feeds for Business 及/或 IBM Security Trusteer Rapport Fraud Feeds for Retail

「客戶」（及其不限數量之授權人員）可使用 TMA 接收有關特定「帳戶持有人」桌面上惡意軟體感染及其他端點漏洞之事件資料。

2.2.2 IBM Security Trusteer Rapport Phishing Protection for Business 及/或 IBM Security Trusteer Rapport Phishing Protection for Retail

「客戶」（及其不限數量之授權人員）可使用 TMA 接收有關將「帳戶持有人」之登入認證提交至可疑之網路釣魚網站或潛在詐欺網站之事件資料通知。合法線上應用程式 (URL) 有可能因錯誤標示而被視為網路釣魚網站，因而致使本 IBM SaaS 向「帳戶持有人」警示某合法網站為網路釣魚網站。發生此情況時，「客戶」應通知 IBM 該項錯誤，IBM 將予以更正。此為「客戶」應為該項錯誤採取的唯一補救措施。

2.2.3 IBM Security Trusteer Rapport Mandatory Service for Business 及/或 IBM Security Trusteer Rapport Mandatory Service for Retail

「客戶」為其「商業應用程式」及/或「零售業應用程式」訂用 IBM SaaS 供應項目涵蓋項目後，便可使用 Trusteer Splash 行銷平台實例，要求將「帳戶持有人用戶端軟體」下載給存取該等應用程式之「合格參與者」。

IBM Security Trusteer Rapport Premium Support for Business 係為 IBM Security Rapport Mandatory Service for Business 之必備項目。

IBM Security Trusteer Rapport Premium Support for Retail 係為 IBM Security Rapport Mandatory Service for Retail 之必備項目。

「客戶」為其「零售業或商業應用程式」訂用 IBM SaaS 供應項目涵蓋項目後，須先訂購 IBM Security Trusteer Rapport Mandatory Service 附加功能，並將其配置為與該應用程式一併使用，始得實作該等附加功能。

3. IBM Security Trusteer Pinpoint 供應項目

IBM Security Trusteer Pinpoint 係為雲端型服務，其設計目的在於提供其他保護層，並以偵測及減輕惡意軟體、網路釣魚及帳戶接管等攻擊為其目標。「客戶」為「客戶」之「商業應用程式」及/或「零售業應用程式」訂用 IBM SaaS 供應項目所涵蓋項目及防詐欺處理程序後，Trusteer Pinpoint 便可整合至該等應用程式。

本 IBM SaaS 供應項目包括：

a. TMA：

   TMA 係於 IBM Security Trusteer 雲端管理之環境中提供，透過此應用程式，「客戶」（及不限數量之授權人員）可執行下列作業：(i) 接收事件資料報告及風險評量；(ii) 檢視、配置及設定安全政策及有關事件資料報告之政策。

b. Web Script 及/或 API：

   用於為存取或使用 IBM SaaS 而部署於網站。

3.1 IBM Security Trusteer Pinpoint Malware Detection 及 IBM Security Trusteer Pinpoint Criminal Detection

若在 IBM Security Trusteer Pinpoint Malware Detection 供應項目中偵測到惡意軟體，或在 IBM Security Trusteer Pinpoint Criminal Detection 供應項目中偵測到帳戶接管，「客戶」應遵循「Pinpoint 實作典範手冊」之指示進行相關處置。請勿於偵測到惡意軟體或帳戶接管後立即以足以影響「合格參與者」使用體驗之方式使用 IBM Security Trusteer Pinpoint Malware Detection 供應項目或 IBM Security Trusteer Pinpoint Criminal Detection 供應項目，因為這樣做會讓他人可以使用 IBM Security Trusteer Pinpoint 供應項目鏈結「客戶」之動作（例如：通知、訊息、封鎖裝置，或在偵測到惡意軟體或帳戶接管後立即封鎖對「商業應用程式」及/或「零售業應用程式」之存取）。

3.1.1 IBM Security Trusteer Pinpoint Criminal Detection for Business 及/或 IBM Security Trusteer Pinpoint Criminal Detection for Retail

可使用裝置 ID、網路釣魚偵測及惡意軟體驅動之認證竊取偵測，對連接至「商業應用程式」或「零售業應用程式」瀏覽器進行無用戶端式可疑帳戶接管活動偵測。IBM Security Trusteer Pinpoint Criminal Detection 供應項目提供其他保護層，且其目標為偵測帳戶接管嘗試，以及將存取「商業應用程式」或「零售業應用程式」之瀏覽器或行動式裝置之風險評量評分直接遞送給「客戶」（透過原生瀏覽器或「客戶」行動式應用程式）。

a. 事件資料：

   「客戶」為其「商業應用程式」及/或「零售業應用程式」訂用 IBM SaaS 供應項目涵蓋項目後，當「合格參與者」與該等應用程式進行線上互動時，便會產生事件資料，此時，「客戶」（及其不限數量之授權人員）可使用 TMA 接收該等事件資料，或者，「客戶」可透過後端 API 遞送模式接收該等事件資料。

3.1.2 IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile 及/或 IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile

IBM Security Trusteer Pinpoint Criminal Detection for Mobile (PPCD Mobile) 供應項目之設計目的，在於提供其他保護層，且其目標在於藉由辨識違法帳戶存取及為「客戶」提出建議，以防範帳戶接管及詐欺活動。「客戶」之使用 PPCD Mobile API 之「商業應用程式」及/或「零售業應用程式」，以及「合格參與者」之行動式裝置，其所提供之資訊均可由本 IBM SaaS 供應項目蒐集。IBM Security Trusteer PPCD Mobile 供應項目之設計目的，在於將「合格參與者」之行動式裝置相關複雜資訊與其他資料來源產生關聯，例如：透過本「使用條款」所載 IBM Security Trusteer 之其他 IBM SaaS 供應項目而整合之即時惡意軟體感染及網路釣魚發生事件。

「客戶」得在 IBM Security Trusteer 之雲端管理環境中存取及使用 IBM Security Trusteer PPCD Mobile 供應項目，此外，「客戶」為其「商業應用程式」或「零售業應用程式」訂用 IBM SaaS 供應項目所涵蓋項目後，「客戶」亦可接收因「合格參與者」之行動式裝置與該等應用程式進行線上互動而產生之風險評量資料。基於本供應項目之目的，「行動式裝置」僅包括支援之行動式電話與平板電腦，不包括 PC 或 MAC。

3.1.3 IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition 及/或 IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition 及/或 IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition 及/或 IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition

可對連接至「商業應用程式」及/或「零售業應用程式」且被「瀏覽器中間人」(Man-in-the-Browser, MitB) 金融業惡意軟體感染之瀏覽器，進行無用戶端式偵測。IBM Security Trusteer Pinpoint Malware Detection 供應項目提供其他保護層，且其目標為將存在 MitB 金融惡意軟體之評量與警示提供予「客戶」，使組織得以依惡意軟體風險，將關注重點放在防詐欺處理程序。

a. 事件資料：

「客戶」（及其不限數量之授權人員）可使用 TMA 接收因「合格參與者」與「客戶」之「商業應用程式」及/或「零售業應用程式」進行線上互動而產生之事件資料。

b. 進階版：

「商業進階版」及/或「零售業進階版」提供其他偵測及保護層，「客戶」可針對其「商業應用程式」及/或「零售業應用程式」之結構與流程調整及客製該層，並可針對以「客戶」為目標之特定威脅趨勢客製該層。該偵測及保護層可併入「客戶」之「商業應用程式」及/或「零售業應用程式」中各個不同位置。

「進階版」適用於「零售業合格參與者」數量達 100K 以上或「商業合格參與者」數量達 10K 以上之「客戶」；即 1000 組的「100 個零售業合格參與者」，或 1000 組的「10 個商業合格參與者」。

c. 標準版：

「商業標準版」或「零售業標準版」係為快速部署解決方案，可提供本 IBM SaaS 供應項目之核心功能，如本合約所規定。

3.2 IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition 及/或 IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition 及/或 IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition 及/或 IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition 適用之選用額外 IBMSaaS 供應項目

IBM Security Trusteer Rapport Remediation for Retail 供應項目之必備項目為 IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition 或 IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition。

IBM Security Trusteer Pinpoint Carbon Copy for Retail 之必備項目為 IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition 或 IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition。IBM Security Trusteer Pinpoint Carbon Copy for Business 之必備項目為 IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition 或 IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition。

3.2.1 IBM Security Trusteer Pinpoint Carbon Copy for Business 及/或 IBM Security Trusteer Pinpoint Carbon Copy for Retail

IBM Security Trusteer Pinpoint Carbon Copy 供應項目之設計目的，在於提供其他保護層及監視服務，以便於「客戶」為其「零售業或商業應用程式」訂用 IBM SaaS 供應項目所涵蓋項目後，因網路釣魚對該等應用程式之攻擊致使「合格參與者」之認證受到危害時協助識別。

3.2.2 IBM Security Trusteer Rapport Remediation for Retail

IBM Security Trusteer Rapport Remediation for Retail 之目標，係於依特定基礎存取「客戶」之「零售業應用程式」之「合格參與者」裝置 (PC/MAC) 受到「瀏覽器中間人」(Man-in-the-Browser, MitB) 惡意軟體感染，而由 IBM Security Trusteer Pinpoint Malware Detection 事件資料偵測到該 MitB 惡意軟體感染後，對其進行調查、補救、封鎖及移除。「客戶」應備有實際執行於「客戶」之「零售業應用程式」之 IBM Security Trusteer Pinpoint Malware Detection 之現行訂用。「客戶」只能與存取「客戶」之「零售業應用程式」之「合格參與者」一起使用本 IBM SaaS 供應項目，且只能將該供應項目當作一種以調查及補救依特定基礎使用之特定受感染裝置 (PC/MAC) 為目標之工具。IBM Security Trusteer Rapport Remediation for Retail 必須實際執行於前項受感染之「合格參與者」裝置 (PC/MAC)，且該等受感染之「合格參與者」必須接受 EULA，且至少使用「客戶」之「零售業應用程式」進行一次鑑別，因此，「客戶」之配置必須包括「使用者 ID」之蒐集。為避免疑慮，特此說明，本 IBM SaaS 供應項目未包含 Trusteer Splash 之使用權，及/或以任何其他方式促銷「帳戶持有人用戶端軟體」，以增加「客戶」之一般「合格參與者」數量之權利。

4. IBM Security Trusteer Mobile 供應項目

4.1 IBM Security Trusteer Mobile Browser for Business 及/或 IBM Security Trusteer Mobile Browser for Retail

IBM Security Trusteer Mobile Browser 之設計目的，在於新增其他保護層，且其目標在於為存取「客戶」之「零售業或商業應用程式」（「客戶」已為該等應用程式訂用 IBM SaaS 供應項目所涵蓋項目） 之「合格參與者」行動式裝置提供安全線上存取，並提供行動式裝置風險評量及網路釣魚防護。安全的 Wi-Fi 偵測僅適用於 Android 平台。基於本 IBM SaaS 供應項目之目的，前項行動式裝置包括行動式電話或平板電腦，但不包括 PC 或 MAC 筆記型電腦。

於「合格參與者」行使下列行為後，「客戶」（及其不限數量之授權人員）可透過 TMA 接收有關該等參與者所用裝置之事件資料、分析及統計資料資訊：(i) 下載「帳戶持有人用戶端軟體」（一種應用程式，其授權係依終端使用者授權合約 ("EULA") 免費提供予大眾，並可供下載至「合格參與者」之行動式裝置）；及 (ii) 接受 EULA，並於「客戶」為其「商業應用程式」或「零售業應用程式」訂用 IBM SaaS 供應項目所涵蓋項目後，至少使用該等應用程式進行一次鑑別。「客戶」僅限使用 Trusteer Splash 行銷「帳戶持有人用戶端軟體」，不得將「帳戶持有人用戶端軟體」使用於其內部業務運作。

a. 事件資料：

   「客戶」為其「零售業或商業應用程式」訂用 IBM SaaS 供應項目涵蓋項目後，「客戶」（及其不限數量之授權人員）便可使用 TMA 接收因行動式裝置與該等應用程式進行線上互動而產生之事件資料。

b. Trusteer Splash：

   「客戶」為其「商業應用程式」及/或「零售業應用程式」訂用 IBM SaaS 供應項目所涵蓋項目後，Trusteer Splash 行銷平台便可對存取該等應用程式之「合格參與者」指明及行銷「帳戶持有人用戶端軟體」。「客戶」得從可用的啟動畫面範本（「啟動畫面範本」）選取其所要範本。客製啟動畫面得依個別簽立之合約或工作說明書提供之。

「客戶」同意得於搭配使用 TMA 時提供「客戶」之商標、標誌或圖示，惟僅限與 Trusteer Splash 搭配使用，且僅限顯示於「帳戶持有人用戶端軟體」或 IBM 所管理之登入頁面，或 IBM Security Trusteer 網站。使用「客戶」所提供之商標、標誌或圖示時，應遵循 IBM 就廣告及商標用法所訂定之合理政策。

4.2 IBM Security Trusteer Mobile SDK for Business 及/或 IBM Security Trusteer Mobile SDK for Retail

IBM Security Trusteer Mobile SDK 供應項目之設計目的，在於新增其他保護層，且其目標在於為「客戶」之「商業應用程式或「零售業應用程式」（「客戶」已為該等應用程式訂用 IBM SaaS 供應項目所涵蓋項目）提供安全的 Web 存取，並提供裝置風險評量及網路釣魚防護。安全的 Wi-Fi 偵測僅適用於 Android 平台。

IBM Security Trusteer Mobile SDK 供應項目包含專有行動式軟體開發者套件 ("SDK")，此軟體套件內含說明文件、程式設計專有軟體程式庫及其他相關檔案與項目（稱為 IBM Security Trusteer 行動式程式庫及「執行時期元件」或「可再散布元件」，此元件係為專有程式碼，由 IBM Security Trusteer Mobile SDK 產生，可內嵌及整合至「客戶」之受保護獨立式 iOS 或 Android 行動式應用程式（「客戶」已為此等應用程式訂用 IBM SaaS 供應項目涵蓋項目）--（「客戶整合行動式應用程式」））。

IBM Security Trusteer Mobile SDK for Retail 係以 100 個「合格參與者」或 100 個「用戶端裝置」為一個套組之方式提供，IBM Security Trusteer Mobile SDK for Business 則以 10 個「合格參與者」或 10 個「用戶端裝置」為一個套組之方式提供。

透過 TMA，「客戶」（及其不限數量之授權人員）可接收事件資料報告及風險趨勢評量。「合格參與者」下載「用戶端整合行動式應用程式」後，「客戶」便可透過「用戶端整合行動式應用程式」接收有關該等參與者行動式裝置之風險分析及行動式裝置資訊，讓「客戶」可針對這些風險制定防詐欺政策以執行規避行動。基於本供應項目之目的，「行動式裝置」僅包括支援之行動式電話與平板電腦，不包括 PC 或 MAC。

「客戶」得執行以下各項：

a. 在其內部使用 IBM Security Trusteer Mobile SDK，惟僅限以開發「用戶端整合行動式應用程式」為目的。

b. 以整體、不可分離之方式將「可再散布元件」（僅限採用物件程式碼格式）內嵌至「用戶端整合行動式應用程式」中。依本授權之規定對「可再散布元件」所為修改或合併之部分，受本「使用條款」之規範。

c. 行銷及散布「可再散布元件」，以供下載至「合格參與者」之行動式裝置或「用戶端裝置持有人」，惟需遵守下列規定：

   - 除非本合約另有明文許可，否則，「客戶」(1) 不得使用、複製、修改或散布 SDK；(2) 不得逆向組合、逆向編譯或以其他方法解譯 SDK，惟法律規定不得以契約限制者，不在此限；(3) 不得再授權或租賃 SDK；(4) 不得移除「可再散布元件」所含任何著作權或注意事項檔案；(5) 不得使用同於原「可再散布元件」檔案/模組之路徑名稱；及 (6) 非經 IBM 或授權人或經銷商事先書面同意，不得結合「用戶端整合行動式應用程式」之行銷而使用 IBM 或該授權人或經銷商之名稱或商標。
   - 「可再散布元件」必須以不可分離之方式整合於「客戶整合行動式應用程式」中。「可再散布元件」僅限採用物件程式碼格式，且需遵循 SDK 及其說明文件中之一切指示與規格。「客戶整合行動式應用程式」之使用者授權合約，必須告知使用者不得對「可再散布元件」行使下列行為：i) 將其使用於非為啟用「客戶整合行動式應用程式」之用途；ii) 將其使用於非為啟用「客戶整合行動式應用程式」之用途；iii) 進行後續之散布或轉讓；iv) 逆向組合、逆向編譯或以其他方法解譯，但法律另有明文規定或不得立約捨棄者，不在此限。「客戶」之授權合約對 IBM 之保護，至少應與本合約之條款相同。
   - SDK 僅限部署於「客戶」指定之行動式測試裝置，以作為「客戶」之內部開發與單元測試之一部分。「客戶」無權將 SDK 用於處理正式作業工作量、模擬正式作業工作量或測試程式碼、應用程式或系統之可調整性。「客戶」無權將 SDK 之任何部分用於任何其他用途。

「客戶整合行動式應用程式」及「客戶」依本合約規定所為之「可再散布元件」修改，其技術協助由「客戶」負責提供。

「客戶」僅限於為支援其對 IBM SaaS 供應項目之使用而安裝及使用「可再散布元件」及 IBM Security Mobile SDK。

IBM 已針對由 IBM Security Trusteer Mobile SDK 所提供之行動式工具（「行動式工具」）建立之應用程式範例進行測試，以判定該等應用程式範例能否適當地執行於 Apple (iOS)、Google (Android) 及其他公司提供之某些版本的行動式作業系統平台（統稱「行動式作業系統平台」），惟行動式作業系統平台係由第三人提供，非 IBM 所能掌控，且亦未於其變更時通知 IBM。因此，不論本合約是否有相反規定，IBM 並未提供下列保證：前項利用「行動式工具」建立的應用程式或其他輸出，可於任何「行動式 OS 平台」或行動式裝置上正常執行、可於該等平台或裝置互相通連或相容。

「客戶」同意建立、保留以下各項資料並將其提供予 IBM 及其稽核員：正確之書面記錄、系統工具輸出及其他足以查核「客戶」使用 IBM Security Trusteer Mobile SDK 時是否遵循本「使用條款」之系統資訊。

5. IBM SaaS Fraud Protection 供應項目之部署

「客戶」之基本程式訂用包含必要設定及初次部署活動，包括初次一次啟動、配置、「啟動畫面範本」、測試及訓練。

額外服務需依個別所簽立合約並收取額外費用後而提供。

附錄 B

IBM 提供 IBM SaaS 之下列可用性服務水準協定 ("SLA")，但僅於「客戶」之「交易文件」中有載明適用時，始適用之：

本 SLA 之版本，係以「客戶」開始訂用或續約訂用時的最新版本為準。「客戶」瞭解本 SLA 不構成對「客戶」提供保證。

1. 定義

a. **授權聯絡人** - 表示「客戶」已向 IBM 指定有權根據此 SLA 提交「請求」的個人。

b. **可用度扣抵** - 係指 IBM 將針對已驗證之「請求」所提供的補救辦法。「可用度扣抵」將針對 貴客戶未來訂用 IBM SaaS 之費用發票，以折抵或折扣方式提供之。

c. **請求 (Claim)** - 係指「客戶」之「授權聯絡人」由於「合約月份」期間未符合「服務水準」，而根據本 SLA 向 IBM 提交的請求。

d. **合約月份** - 係指 IBM SaaS 實施期間的每個完整月份，從當月第一天的格林威治標準時間 (GMT) 上午 12:00 算起，直到當月最後一天的 GMT 下午 11:59 為止。

e. **「客戶」**係指直接向 IBM 訂用 IBM SaaS 的實體，且未違反其與 IBM 訂定的 IBM SaaS 合約之重要義務（含付款義務）。

f. **停用時間** - 係指處理「服務」的正式作業系統已停止的時段，而且所有 貴客戶的使用者無法使用他們有適當許可權之「服務」的全部功能。「停用時間」並不包括由於下列情況而無法使用的時段：

- 計劃的系統停用時間；
- 不可抗力；
- 「客戶」或第三人應用程式、設備或資料發生問題；
- 客戶或第三人的行為或疏忽（包括任何人藉由「客戶」的密碼或設備存取 IBM SaaS）；
- 未遵守存取 IBM SaaS 所需的系統配置及支援平台；或
- IBM 遵照「客戶」或代表「客戶」之第三人所提供的任何設計、規格或指示所為者。

g. **事件** - 係指一種情況或一組一起發生的情況，導致無法符合「服務水準」。

h. **不可抗力** - 係指天災、恐怖活動、勞工行動、火災、水災、地震、暴動、戰爭、政府行政行為、命令或限制、病毒、阻斷服務攻擊及其他惡意行為、公用事業及網路連線失敗，或任何其他超出 IBM 合理控制而無法使用 IBM SaaS 的原因。

i. **「計劃性的系統停用時間」** - 係指基於維護目的而預定的 IBM SaaS 停止時間。

j. **服務水準** - 係指如下所述之標準，IBM 依照該標準，來計算其在本 SLA 中所提供的服務水準。

2. 可用度扣抵

a. 為了有資格提交「請求」，「客戶」應已根據報告「嚴重性層級 1」支援問題的 IBM 程序，針對適用 IBM SaaS，利用 IBM 客戶支援中心服務台記載每一個「事件」的支援問題單。「客戶」應提供有關「事件」的所有必要詳細資訊，並以「嚴重性 1」支援問題單所需的程度，適度地協助 IBM 診斷及解決「事件」。「客戶」應在一開始得知「事件」已影響「客戶」使用 IBM SaaS 的二十四 (24) 小時內記載此等問題單。

b. 在以「請求」事由發生之「合約月份」結束之後，「客戶」的「授權聯絡人」應於三 (3) 個營業日內提交「客戶的可用度扣抵請求」。

c. 「客戶」的「授權聯絡人」必須提供給 IBM 所有關於「請求」的合理詳細資料，包括但不限於所有相關「事件」的詳細說明，以及未符合的「服務水準」。

d. IBM 將在內部計算適用於下表顯示之對應「服務水準」的每一個「合約月份」期間的總累積計算之「停用時間」。「可用度扣抵」將根據從「客戶」報告第一次受到「停用時間」影響的時間算起的「停用時間」期間。如果「客戶」報告「應用程式停用時間事件」及「入埠資料處理停用時間事件」同時發生，則 IBM 將把重疊的「停用時間」期間視為單一「停用時間」期間，而非視為兩個分別的「停用時間」期間。對於每一個有效的「請求」，IBM 將依每一個「合約月份」期間達成的「服務水準」，選擇最高可適用的「可用度扣抵」，如下表所示。 IBM 將不對相同「合約月份」中之相同「事件」重複提供多個「可用度扣抵」。

e. 對於個別 IBM SaaS 被一起包裝並以單一結合價格販售之「組合服務」，IBM 將根據「組合服務」的單一結合每月價格來計算「可用度扣抵」，而非以每個個別 IBM SaaS 的每月訂用費用計算之。「客戶」只能提交與任何「合約月份」中一個組合內某個個別 IBM SaaS 相關的「請求」，而且 IBM 將不會對任何「合約月份」中一個組合內的多個 IBM SaaS 提供超過一個的「可用度扣抵」。

f. 若「客戶」已在轉銷交易中從合格的 IBM 轉銷商購得 IBM SaaS，而在此交易中，IBM 係負起履行 IBM SaaS 及 SLA 承諾的主要責任時，則「可用度扣抵」將根據「請求」所主張之「合約月份」的有效 IBM SaaS 之當時「關係建議報價 (RSVP)」，折扣率為 50%。

g. 在任何情況下，於任何「合約月份」中，IBM 所提供之「可用度扣抵」總計以「客戶」取得 IBM SaaS 而支付給 IBM 之年費的十二分之一 (1/12) 的百分之十 (10%) 金額為扣抵上限。

h. IBM 將使用其合理的判斷，根據 IBM 記錄中的可用資訊來驗證「請求」，如果此資訊與「客戶」記錄中的資料發生牴觸，將優先適用 IBM 記錄中的資訊。

i. 根據此 SLA 提供給「客戶」的可用度扣抵是與任何請求有關的唯一且排除其他之補救辦法。

3. 服務水準

合約月份期間的 IBM SaaS 可用度

達成的服務水準 **（在「合約月份」期間）**	**可用度扣抵** **（以「請求」之項目之「合約月份」的「每月訂用費用」百分比）**
< 99.5%	2%
< 98.0%	5%
< 96.0%	10%

「達成的服務水準」（以百分比表示）會計算為：(a)「合約月份」中的總分鐘數減去 (b)「合約月份」中「停用時間」的總分鐘數，除以 (c)「合約月份」的總分鐘數。

範例：「合約月份」期間的「停用時間」總共 250 分鐘

30 天「合約月份」，總共 43,200 分鐘 - 停用時間 250 分鐘 = 42,950 分鐘 總共 43,200 分鐘	= 「合約月份」期間的達成服務水準達 99.4% 時為 2% 可用度扣抵

3.1 除外條款

本 SLA 只適用於「IBM 客戶」。本 SLA 不適用於下列情況：

- 測試版及試用版服務。
- 非正式作業環境，包括且不限於測試、災難回復、品質保證或開發。
- 由「IBM 客戶」的使用者、來賓、參與者及允許的 IBM SaaS 受邀者所提出的「請求」。
- 「客戶」違反本「使用條款」規定之重要義務，包括但不限於違反付款義務。