IBM Trusteer Pinpoint Detect

本「服務說明」說明本「雲端服務」之內容。適用之訂購文件提供 貴客戶訂單有關計價及其他詳細資料。

1. 雲端服務

IBM 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。 貴客戶為 貴客戶之「商業應用程式」及/或「零售業應用程式」訂用「雲端服務」涵蓋項目及防詐騙處理程序後，Trusteer Pinpoint 便可整合至該等應用程式。

本「雲端服務」包括：

a. Trusteer 管理應用程式 (TMA) 及 Trustboard：

TMA 為 Trusteer 之傳統管理應用程式，可讓 貴客戶對警示進行評量與分類。Trustboard 為主要用於研究之較新管理應用程式。貴客戶一次僅得選用 TMA 或 Trustboard 其中之一。TMA 及 Trustboard 係於 IBM Trusteer 雲端代管之環境中提供，透過此應用程式， 貴客戶（及不限數量之其授權人員）可執行下列作業：(i) 檢視及下載若干事件資料之報告及風險評估；及 (ii) 檢視、訂用及配置從 Pinpoint 供應項目所產生威脅資訊來源之遞送。IBM Trusteer Pinpoint Detect 及 IBM Trusteer Pinpoint Verify 係作為 TMA 及 Trusteer 登入之一部分。

b. Web Script 及/或 API：

用於為存取、測試或使用本「雲端服務」而部署於網站。

「階段作業」為「用戶端應用程式」（Web 或行動式）與產生一或多項即時風險評量之「雲端服務」二者間之互動。「階段作業」之時間計量，自互動開始起算，至互動結束止。於發生下列其中一項時，記錄互動之結束：

- 以一般登出應用程式之方式重設互動。
- 瀏覽器、應用程式或標籤已關閉。
- 刪除 Cookie。
- 逾時。

「階段作業」可能包含任意數量之活動，例如：登入、瀏覽、結帳、付款設定及其他由「用戶端應用程式」定義之活動。為求明確，茲進一步說明如下：基於本「雲端服務」之目的，一個「連線」（如下所定義者）為一個「階段作業」。

1.1 供應項目

貴客戶得從下列可用供應項目選取其所要供應項目。

1.1.1 IBM Trusteer Pinpoint Detect Standard for Retail 及/或 IBM Trusteer Pinpoint Detect Standard for Business

本項「雲端服務」結合 IBM Trusteer Pinpoint Criminal Detection 及 IBM Trusteer Pinpoint Malware Detection 二項「雲端服務」，提供單一統合之解決方案。

本解決方案有助於使用裝置 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「零售業應用程式」或「商業應用程式」之瀏覽器進行無用戶端式惡意軟體及/或可疑帳戶接管活動偵測。IBM Trusteer Pinpoint 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「零售業應用程式」或「商業應用程式」之瀏覽器或行動式裝置之風險評量評分直接遞送給 貴客戶（透過原生瀏覽器或 貴客戶行動式應用程式）。本「服務」亦得用於遠端人力存取，以評量受管理與未受管理裝置所生風險。

本「雲端服務」包含頂級支援（如以下「技術支援」一節所定義者）。

本項服務之購買，以「100 位合格參與者」或「100 個連線」為一套組。

1.1.2 IBM Trusteer Pinpoint Detect Premium for Retail 及/或 IBM Trusteer Pinpoint Detect Premium for Business

本項「雲端服務」結合 IBM Trusteer Pinpoint Criminal Detection 及 IBM Trusteer Pinpoint Malware Detection，提供容易整合之單一統合解決方案。

本解決方案有助於使用裝置 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「零售業應用程式」或「商業應用程式」之瀏覽器進行無用戶端式惡意軟體及/或可疑帳戶接管活動偵測。IBM Trusteer Pinpoint 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 貴客戶（透過原生瀏覽器或 貴客戶行動式應用程式）。

本項服務包含加強的功能和服務，包括：延伸的部署及設定服務、客製之安全政策、調查服務等。本項服務於進行設定時，最多包含每一應用程式上限 200 小時部署服務共用資源，以及每一應用程式上限 200 小時安全分析共用資源。後續服務包括每一應用程式每年上限 20 小時部署維護，以及每一應用程式每年上限 100 小時安全研究。額外服務項目應另外付費。

Pinpoint Detect 會從「行動式」通道及 Web 通道耗用交易。若包含「行動式」交易，則適用按「連線」購買之 Pinpoint。本項「雲端服務」包含保護一個「應用程式」。「客戶」應就各額外「應用程式」取得 IBM Trusteer Pinpoint Detect Premium Additional Applications 之授權。

本項「雲端服務」包含頂級支援。

IBM Trusteer Pinpoint Detect Premium for Retail and Business 服務之購買，以「100 位合格參與者」為一套組，如係為 IBM Trusteer Pinpoint Detect Premium 者，以「100 個連線」為一套組。「客戶」選擇按「連線」購買服務者，自第一個應用程式起即需收取 Additional Application 費用。

Pinpoint Detect Policy Manager：

Policy Manager 包含在 Pinpoint Detect Premium 服務中，於 IBM Trusteer 雲端代管之環境中提供， 貴客戶（及不限數量之授權人員）可透過它來執行下列作業：(i) 設計、測試及部署至正式作業環境邏輯以偵測詐騙活動，(ii) 設計報告和儀表板，(iii) 檢視、配置及設定安全政策及用來偵測客戶「應用程式」之可疑活動的政策。

若要啟動 Policy Manager 特定功能 (features) 及獲得額外深入探究之必要支援，需要有諮詢服務。我們將另外在工作說明書中約定諮詢服務詳細內容。

當 Policy Manager 啟動後，基於支援目的，IBM 保留存取 貴客戶環境以調整 貴客戶原則之權利，重新修補因原則變更所衍生之重大議題。

「客戶」承諾會保護經由 Policy Manager 公開之任何資料，免於被不當使用。

當 Policy Manager 特定功能啟動後， 貴客戶必須遵循 IBM 準則進行規則設定，如說明文件中所約定。貴客戶確認，IBM 對於 貴客戶未遵循建議而可能衍生之任何狀況概不負責。

任何因 貴客戶將 Policy Manager 特定功能配置錯誤而可能產生之穩定性及/或服務降級問題，在 SLA 計算中不會被視為停用時間。

1.1.3 IBM Trusteer Pinpoint Detect for Connections

本「雲端服務」提供保護功能，且其目標為偵測帳戶接管嘗試，以及遞送存取「商業」或「零售業」應用程式之瀏覽器及/或行動式裝置之風險/信賴評量評分（透過 貴客戶行動式應用程式之原生瀏覽器）。本解決方案利用各種風險指標分析終端使用者之裝置、連線及行為，並將其與使用者歷程做比較，以確認可疑使用情形。

本「雲端服務」會從「行動式」通道及 Web 通道耗用連線。IBM Trusteer Pinpoint Detect 包含相關 IBM Trusteer Mobile SDK 之授權。

本「雲端服務」係以每年 100 個「連線」為一套組之方式購買之。

1.1.4 IBM Trusteer Pinpoint Detect Bundle

本「雲端服務」軟體組係由 IBM Trusteer Pinpoint Detect、IBM Trusteer Mobile SDK 及 IBM Trusteer Rapport 提供。本「雲端服務」提供保護功能，且其目標為偵測帳戶接管嘗試，以及遞送存取「商業」或「零售業」應用程式之瀏覽器及/或行動式裝置之風險/信賴評量評分（透過 貴客戶行動式應用程式之原生

瀏覽器）。本解決方案利用各種風險指標分析終端使用者之裝置、連線及行為，並將其與使用者歷程做比較，以確認可疑使用情形。

本服務係按「作用中使用者」購買之。

本「雲端服務」會從「行動式」通道及 Web 通道耗用連線。IBM Trusteer Pinpoint Detect 包含對 IBM Trusteer Mobile SDK 之存取權限。

IBM Trusteer Pinpoint Detect Bundle 包含對 IBM Trusteer Rapport 之存取權限。除 IBM 另以書面載明者外，前揭存取權限包括 Trusteer Splash 和 IBM Trusteer Rapport Mandatory Service。

IBM Trusteer Mobile SDK

IBM Trusteer Mobile SDK「雲端服務」之設計目的，在於新增其他保護層，且其目標在於為 貴客戶之「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「雲端服務」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 Trusteer Mobile SDK「雲端服務」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 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 Trusteer Mobile SDK 產生，可內嵌及整合至 貴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雲端服務涵蓋項目）-（「客戶整合行動式應用程式」））。

貴客戶得執行以下各項：

a. 在其內部使用 IBM 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「服務說明」之條款所拘束。

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

   - 除非本合約另有明文許可，否則， 貴客戶(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拋棄者，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」之終端使用者授權合約 ("EULA")，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契約拋棄者，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 貴客戶指定之行動式測試裝置，以作為 貴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」應自行負責「客戶整合行動式應用程式」之部署、測試及支援。「客戶整合行動式應用程式」及貴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 貴客戶負責提供。

限於為支援其對「雲端服務」之使用， 貴客戶被授權得安裝及使用「可再散布元件」及 IBM Security Mobile SDK。

IBM 不為下列保證：利用 IBM Security Mobile SDK 隨附行動式工具建立之應用程式或產出，必能與特定行動式作業系統平台或行動式裝置搭配運作、互相通連或相容。

「原始碼元件」(Source Components) 及「範例著作物」(Sample Materials) - IBM Trusteer Mobile SDK 可能包含採用某些原始碼元件（「原始碼元件」）及識別為「範例著作物」之其他著作物 (material)。「客

戶」僅限於本「合約」之授權權利限制規定範圍內，供內部使用而複製及修改「原始碼元件」及「範例著作物」；惟 貴客戶不得變更或刪除「原始碼元件」或「範例著作物」所含之任何著作權資訊或通知。 IBM 依「現狀」提供「原始碼元件」及「範例著作物」，且不負支援之義務。請注意：「原始碼元件」及「範例著作物」僅供作為範例，用以示範如何將「可內嵌元件」實作至 CIMA 中。「原始碼元件」或「範例著作物」可能與 貴客戶之開發環境不相容。「客戶」應自行負責測試「可內嵌元件」，並將其實作至其 CIMA 中。

若本服務說明項下「雲端服務」係由 International Business Machines Corporation（紐約公司 - "IBM Corporation"）提供，則適用本段落中之下列規定。本服務說明項下 SDK 與「可再散布元件」之權利，係由 IBM Corporation 授與。IBM 係作為散布者，依本合約規定交付 SDK 與「可再散布元件」，並負責履行該等 SDK 與「可再散布元件」有關授權條款及一切義務，且依本服務說明規定並無有關有利於 貴客戶而不利於 IBM Corporation 之權利或訴因。 貴客戶拋棄對 IBM Corporation 提出一切請求及訴因之權利，並同意僅就 SDK 與「可再散布元件」對 IBM 要求權利及救濟。

IBM 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 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 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「雲端服務」供應項目包括：

a. Web Script：

用於為存取、測試或使用本「雲端服務」而於網站上進行存取。

1.2 選用服務

本節中之「雲端服務」，其必備項目為 IBM Trusteer Pinpoint Detect Premium、IBM Trusteer Pinpoint Detect Standard、IBM Trusteer Pinpoint for Connections 或 IBM Trusteer Pinpoint Detect Bundle 之授權。

1.2.1 IBM Trusteer Pinpoint Detect Standard Application

「用戶端應用程式」係指「Web 應用程式」及/或「行動式應用程式」。「Web 應用程式」對於從登入或識別畫面，透過數個網頁提供給 貴客戶之「合格參與者」，且將其當作單一 Trusteer 主控台（「Trusteer 管理應用程式」）中之單一「應用程式」而予以監視之所有功能，會予以分組。「Mobile 應用程式」對於從登入或識別畫面，透過一個軟體（可從應用程式商店（商店）下載）提供給 貴客戶之「合格參與者」，且將其當作單一 Trusteer 主控台（「Trusteer 管理應用程式」）中之單一「應用程式」而予以監視之所有功能，會予以分組。

必須就每一「應用程式」取得 IBM Trusteer Pinpoint Application 之授權，始得整合 IBM Trusteer Pinpoint。

- 必須就每一「應用程式」取得 IBM Trusteer Pinpoint Detect Standard ApplicationIBM Trusteer Pinpoint Detect Standard Application 之授權，始得部署 IBM Trusteer Pinpoint Detect Standard。

1.2.2 IBM Trusteer Pinpoint Detect Premium Application

「用戶端應用程式」係指「Web 應用程式」及/或「行動式應用程式」。「Web 應用程式」對於從登入或識別畫面，透過數個網頁提供給 貴客戶之「合格參與者」，且將其當作單一 Trusteer 主控台（「Trusteer 管理應用程式」）中之單一「應用程式」而予以監視之所有功能，會予以分組。「Mobile 應用程式」對於從登入或識別畫面，透過一個軟體（可從應用程式商店（商店）下載）提供給 貴客戶之「合格參與者」，且將其當作單一 Trusteer 主控台（「Trusteer 管理應用程式」）中之單一「應用程式」而予以監視之所有功能，會予以分組。

本項服務於進行設定時，最多包含每一應用程式上限 200 小時部署服務共用資源，以及每一應用程式上限 200 小時安全分析共用資源。後續服務包括每一應用程式每年上限 20 小時部署維護，以及每一應用程式每年上限 100 小時安全研究。

- 必須就每一「應用程式」取得 IBM Trusteer Pinpoint Detect Premium Application for every Application 之授權，始得部署 IBM Trusteer Pinpoint Premium。

1.2.3 IBM Trusteer New Account Fraud for Retail 及/或 IBM Trusteer New Account Fraud for Business

本服務（提供予 Pinpoint 訂用者）之設計，目的在於在進行新帳戶建立程序時得以早期偵測異常狀況、標示可疑活動及產生警示。本服務會監測新帳戶，以識別有關建立詐欺貼文帳戶及青年帳戶特性蒐集之新活動，俾以透過 TMA 中所提供之使用報告提供早期警告符號，表示新帳戶可能為錢騾帳戶或可能用於進行詐欺活動。

IBM Trusteer New Account Fraud for Retail 及 IBM Trusteer New Account Fraud for Business 係以 10 次「API 呼叫」為一套組之方式提供。

1.2.4 IBM Trusteer Digital Content Pack for Retail 及/或 IBM Trusteer Digital Content Pack for Business

IBM Trusteer Digital Content Pack 可讓安全分析師整合新的詐騙模型，並同時為特定模型之建立及修改提供完整支援，以因應不斷進展之威脅。本項服務包含一組廣泛之規則、洞察及政策，採購此等規則、洞察及政策後，得將之當作解決方案之一件額外部分及構件。Digital Content Pack 有助於使 Trusteer 之數位防詐騙功能與 IBM Safer Payments 無現金付款通道間之整合更加緊密。Digital Content Pack 可運用其內建規則及特定商業邏輯，協助銀行及其他金融機構提升現有之詐欺偵測和防範功能。

IBM Trusteer Digital Content Pack for Retail 之提供，係以每份 100 位「合格參與者」為計量單位。IBM Trusteer Digital Content Pack for Business 之提供，係以每份 10 位「合格參與者」為計量單位。

Digital Content Pack with Pinpoint Detect 與 IBM Safer Payments 之整合，以及需要特別關注之支援服務，均需要「諮詢」服務。「諮詢」服務應另行簽署個別工作說明書而另外購得。

1.2.5 IBM Trusteer Pinpoint Malware Detection

若在 IBM Trusteer Pinpoint Malware Detection II 雲端服務中偵測到惡意軟體， 貴客戶應遵循《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 Trusteer Pinpoint Malware Detection II 雲端服務，以免遭人利用 IBM Trusteer Pinpoint 雲端服務鏈結 貴客戶之動作（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）。

1.2.6 IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business 及/或 IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail 及/或 IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business 及/或 IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail

IBM Security Pinpoint Malware Detection II 為 IBM Trusteer Pinpoint Malware Detection 之新建構項目，有助於將多個「應用程式」保護相關費用標準化，並取代於新增「應用程式」時所生一次性費用。

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 Trusteer Pinpoint Malware Detection 雲端服務提供其他保護層，且其目標為將存在 MitB 金融惡意軟體之評量與警示提供予 貴客戶，使組織得以依惡意軟體風險，將關注重點放在防詐騙處理程序。

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. Advanced Edition：

   「商業進階版」及/或「零售業進階版」提供其他偵測及保護層， 貴客戶可針對其「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 貴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 以上之貴客戶；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. Standard Edition：

   「商業標準版」及/或「零售業標準版」係為快速部署解決方案，可提供本「雲端服務」之核心功能，如本合約所規定。

本項「雲端服務」包含保護一個「應用程式」。「客戶」應就各額外「應用程式」取得 IBM Trusteer Pinpoint Malware Detection Additional Applications 之授權。

1.2.7 IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail 及/或 IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail 及/或 IBM Pinpoint Trusteer Pinpoint Malware Detection Standard Edition II for Business 及/或 IBM Trusteer Pinpoint Malware Detection Advanced Edition II for BusinessAdvanced Editions for Business 適用之選用額外「雲端服務」

- IBM Trusteer Rapport Remediation for Retail 雲端服務之必備項目為 IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail 或 IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail。
- IBM Trusteer Rapport Remediation for Business 雲端服務之必備項目為 IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business 或 IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business。

1.2.8 IBM Trusteer Pinpoint Criminal Detection for Business 及/或 IBM 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 Trusteer Pinpoint Criminal Detection 雲端服務提供其他保護層，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 貴客戶（透過原生瀏覽器或 貴客戶行動式應用程式）。

a. 事件資料：

貴客戶一次僅得選用 TMA 或 Trustboard 其中之一。貴客戶為其「商業應用程式」及/或「零售業應用程式」訂用本「雲端服務」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， 貴客戶（及其不限數量之授權人員）可使用 TMA 或 Trustboard 接收該等事件資料，或者， 貴客戶可透過後端 API 遞送模式接收該等事件資料。

1.2.9 IBM Trusteer Pinpoint Criminal Detection II for Business 及/或 IBM Trusteer Pinpoint Criminal Detection II for Retail

IBM Security Pinpoint Criminal Detection II 為 IBM Trusteer Pinpoint Criminal Detection 之新建構項目，有助於將多個「應用程式」保護相關費用標準化，並取代於新增「應用程式」時所生一次性費用。

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 Trusteer Pinpoint Criminal Detection II 雲端服務提供其他保護層，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 貴客戶（透過原生瀏覽器或 貴客戶行動式應用程式）。

a. 事件資料：

貴客戶一次僅得選用 TMA 或 Trustboard 其中之一。貴客戶為其「商業應用程式」及/或「零售業應用程式」訂用本「雲端服務」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， 貴客戶（及其不限數量之授權人員）可使用 TMA 或 Trustboard 接收該等事件資料，或者， 貴客戶可透過後端 API 遞送模式接收該等事件資料。

本項「雲端服務」包含保護一個「應用程式」。「客戶」應就各額外「應用程式」取得 IBM Trusteer Pinpoint Criminal Detection Additional Applications 之授權。

1.2.10 IBM Trusteer Rapport Remediation for Retail 及/或 IBM Trusteer Rapport Remediation for Business

IBM Trusteer Rapport Remediation for Retail 及 IBM Trusteer Rapport Remediation for Business 之目標，係於依特定基礎存取 貴客戶之「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 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。 貴客戶應備有實際執行於 貴客戶之「應用程式」之 IBM Trusteer Pinpoint Malware Detection II 之現行訂用。 貴客戶僅限與存取 貴客戶之「應用程式」之「合格參與者」一起使用本「雲端服務」供應項目，且僅限將其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 Trusteer Rapport Remediation 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 貴客戶之「應用程式」進行至少一次鑑別，因此， 貴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，本項「雲端服務」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 貴客戶之一般「合格參與者」數量之權利。基於本「服務說明」之目的，「帳戶持有人」係指 貴客戶之「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 貴客戶之「零售業應用程式」或「商業應用程式」（貴客戶已為該應用程式訂用「雲端服務」涵蓋項目）進行至少一次鑑別。「帳戶持有人用戶端軟體」係指 IBM Trusteer Rapport 用戶端啟用軟體或其他為安裝於終端使用者裝置而隨附於若干「雲端服務」之任何用戶端啟用軟體。

1.2.11 IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail 及/或 IBM Trusteer Pinpoint Malware Detection Additional Applications for Business

- 必須取得 IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail 之授權，始得於第一個「應用程式」以外之額外「零售業應用程式」上部署 IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail 或 IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail。
- 必須取得 IBM Trusteer Pinpoint Malware Detection Additional Applications for Business 之授權，始得於第一個「應用程式」以外之額外「商業應用程式」上部署 IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business 或 IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business。

1.2.12 IBM Trusteer Rapport for Mitigation for Retail 及/或 IBM Trusteer Rapport for Mitigation for Business

- IBM Trusteer Rapport for Mitigation for Retail 之目標，係於依特定基礎存取 貴客戶之「零售業應用程式」之「合格參與者」裝置 (PC/MAC) 受到惡意軟體感染，而由 IBM Trusteer Pinpoint Detect Premium 或 IBM Trusteer Pinpoint Detect Standard 事件資料偵測到該惡意軟體感染後，對其進行調查、補救、封鎖及移除。 貴客戶應備有實際執行於 貴客戶之「零售業應用程式」之 IBM Trusteer Pinpoint Detect Premium 或 IBM Trusteer Pinpoint Detect Standard 之現行訂用。 貴客戶僅限與存取 貴客戶之「零售業應用程式」之「合格參與者」一起使用本項「雲端服務」，且僅限將其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 Trusteer Rapport for Mitigation 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 貴客戶之「零售業應用程式」進行至少一次鑑別，因此， 貴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「雲端服務」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。
- IBM Trusteer Rapport for Mitigation for Business 之目標，係於依特定基礎存取 貴客戶之「商業應用程式」之「合格參與者」裝置 (PC/MAC) 受到惡意軟體感染，而由 IBM Trusteer Pinpoint Detect Premium 或 IBM Trusteer Pinpoint Detect Standard 事件資料偵測到該惡意軟體感染後，對其進行調查、補救、封鎖及移除。 貴客戶應備有實際執行於 貴客戶之「商業應用程式」之 IBM Trusteer Pinpoint Detect Premium 或 IBM Trusteer Pinpoint Detect Standard 之現行訂用。 貴客戶僅限與存取 貴客戶之「商業應用程式」之「合格參與者」一起使用本項「雲端服務」，且僅限將其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 Trusteer Rapport for Mitigation for Business 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 貴客戶之「商業應用程式」進行一次鑑別，因此，貴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「雲端服務」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。

1.2.13 IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail 及/或 IBM Trusteer Pinpoint Detect Standard Additional Applications for Business

- 必須取得 IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail 之授權，始得於第一個「應用程式」以外之額外「零售業應用程式」上部署 IBM Trusteer Pinpoint Detect Standard for Retail。
- 必須取得 IBM Trusteer Pinpoint Detect Standard Additional Applications for Business 之授權，始得於第一個「應用程式」以外之額外「商業應用程式」上部署 IBM Trusteer Pinpoint Detect Standard for Business。

1.2.14 IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail 及/或 IBM Trusteer Pinpoint Detect Premium Additional Applications for Business

本項服務於進行設定時，最多包含每一應用程式上限 200 小時部署服務共用資源，以及每一應用程式上限 200 小時安全分析共用資源。後續服務包括每一應用程式每年上限 20 小時部署維護，以及每一應用程式每年上限 100 小時安全研究。

- 必須取得 IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail 之授權，始得於第一個「應用程式」以外之額外「零售業應用程式」上部署 IBM Trusteer Pinpoint Premium for Retail。
- 必須取得 IBM Trusteer Pinpoint Detect Premium Additional Applications for Business 之授權，始得於第一個「應用程式」以外之額外「商業應用程式」上部署 IBM Trusteer Pinpoint Premium for Business。

1.2.15 IBM Trusteer Pinpoint Detect Standard for Retail Premium Support 及/或 IBM Trusteer Pinpoint Detect Standard for Business Premium Support

「客戶」有購買 Pinpoint Detect Standard 雲端服務者，得購買 Premium Support 服務。Premium Support 服務之範圍載明於以下第 4 節。

1.2.16 IBM Trusteer Mobile Carrier Intelligence for Pinpoint Detect

貴客戶訂用本項「雲端服務」前，必須先備有 IBM Trusteer Pinpoint Detect 之現行訂用。

本「雲端服務」藉由提供有關提供予 IBM Trusteer Pinpoint Detect 之行動電話號碼之額外資訊及環境定義，加強 IBM Trusteer Pinpoint Assure 及/或 IBM Trusteer Pinpoint Detect，以利判斷特定階段作業之詐欺風險。「客戶」得查詢本「雲端服務」，以獲知特定行動電話號碼之特徵，例如：該號碼相關行動通訊業者資訊。

本「雲端服務」所提供有關前揭行動電話號碼之資料（「行動電話情報」）僅得使用於 貴客戶之內部用途，且僅限保留三十 (30) 日。逾前揭保留期限後， 貴客戶須重新查詢本「雲端服務」，以取得有關前揭號碼之「行動電話情報」，不得直接重新使用從前一個查詢收到之「行動電話情報」。除經前揭規定許可外， 貴客戶不得搭配資料採集之全部或一部一併快取、重新使用或使用「行動電話情報」，亦不得保存「行動電話情報」。

1.3 Acceleration Services

1.3.1 IBM Trusteer Pinpoint Detect Standard Redeployment 及/或 IBM Trusteer Pinpoint Detect Premium Redeployment

於服務期間重新部署線上銀行應用系統，並於其後要求變更 IBM Trusteer Pinpoint Detect 部署之 貴客戶，應購買 IBM Trusteer Pinpoint Detect Redeployment。

「重新部署」有可能是因 貴客戶變更「應用程式」之網域或主機 URL，而將線上「應用程式」轉換成新技術、移至新線上銀行平台，或將新登入流程新增至現有「應用程式」。

於 6 個月之重新部署轉移期間內， 貴客戶有權以一對一之方式使用在已訂用「應用程式」上執行之額外「應用程式」。

1.3.2 IBM Trusteer Pinpoint Malware Detection Redeployment

於服務期間重新部署線上銀行應用系統，並於其後要求變更 IBM Trusteer Pinpoint Malware Detection II 部署之 貴客戶，應購買 IBM Trusteer Pinpoint Malware Detection Redeployment。

「重新部署」有可能是因 貴客戶變更「應用程式」之網域或主機 URL，而將線上「應用程式」轉換成新技術、移至新線上銀行平台，或將新登入流程新增至現有「應用程式」。

於 6 個月之重新部署轉移期間內， 貴客戶有權以一對一之方式使用在已訂用「應用程式」上執行之額外「應用程式」。

就 IBM Trusteer Pinpoint Malware Detection II Standard Edition 或 IBM Trusteer Pinpoint Malware Detection II Advanced Edition 適用之 IBM Trusteer Pinpoint Malware Detection Additional Applications，於第一個「應用程式」以外任何額外「應用程式」上所為之部署，均需備有 IBM Trusteer Pinpoint Malware Detection Additional Applications 之授權。

1.3.3 IBM Trusteer Pinpoint Criminal Detection Redeployment

於服務期間重新部署線上銀行應用系統，並於其後要求變更 IBM Trusteer Pinpoint Criminal Detection 雲端服務部署之 貴客戶，應購買 IBM Trusteer Pinpoint Criminal Detection Redeployment。

「重新部署」有可能是因 貴客戶變更「應用程式」之網域或主機 URL，而將線上「應用程式」轉換成新技術、移至新線上銀行平台，或將新登入流程新增至現有「應用程式」。

於 6 個月之重新部署轉移期間內， 貴客戶有權以一對一之方式使用在已訂用「應用程式」上執行之額外「應用程式」。

2. 資料處理及保護 Data Sheet

「IBM 之資料處理附錄」（網址：http://ibm.com/dpa）(DPA) 及 Data Processing and Protection Data Sheet（稱為 Data Sheet 或「DPA 附件」）（如以下鏈結所示）提供有關「雲端服務」之其他資料保護資訊，以及有關可能處理之「內容」類型、所涉及之處理活動、資料保護特定功能 (features) 及「內容」保留與歸還相關細節等事宜之選項。若適用 i) 歐洲一般資料保護規章 (EU/2016/679) (GDPR)；或 ii) http://ibm.com/dpa/dpl 所載明之其他資料保護法，則於其適用的範圍內，「內容」(Content) 所含個人資料適用前揭 DPA。

為求明確，茲進一步說明如下：Data Sheet 通常會列出 IBM（包括第三方再處理者）代管及處理「個人資料」所在之一切位置，不問從中部署服務之資料中心，均同。有關從中部署服務之資料中心特定代管及處理位置之清單，請參閱以下第 5.2 節（「其他處理位置資訊」）。

IBM Trusteer Pinpoint Criminal Detect

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=1402489853624

IBM Trusteer Pinpoint Detect

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=3D3DA0C0E5F711E5A3808DA17FABE9B1

IBM Trusteer Pinpoint Malware Detection

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=1402489595035

IBM Trusteer Mobile SDK

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=1402492847439

IBM Trusteer Rapport

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=1402483908375

3. 服務水準及技術支援

3.1 服務水準協定

IBM 為 貴客戶提供下列可用度服務水準協定 (SLA)。 IBM 將就本「雲端服務」累計可用度依最高可適用度進行補償，如下表所示。可用度百分比之計算方式如下：合約月份中的總分鐘數減去合約月份中「服務停用」之總分鐘數，除以合約月份之總分鐘數。「服務停用」定義、請求的處理及如何洽詢 IBM 有關服務可

用度問題，載明於「IBM 雲端服務」支援手冊（網址：https://www.ibm.com/software/support/saas_support_overview.html）。

可用性	扣抵 （每月訂用費用之 %*）
小於 99.9%	2%
小於 99.0%	5%
小於 95.0%	10%

* 訂用費用為請求所主張當月之約定價格。

3.2 技術支援

於 IBM 支援手冊（網址：https://www.ibm.com/support/home/pages/support-guide/）中選取本「雲端服務」，即可找到本「雲端服務」之技術支援（包括支援聯絡人詳細資料、嚴重性層次、可用支援時數、回應時間及其他支援資訊與處理程序）。

頂級支援：

「頂級支援」訂用項目適用於本「雲端服務」，惟需額外費用，且包括：

- 為所有嚴重性的問題提供全年無休支援。
- 貴客戶可直接透過電話及回電申請取得支援。
- 貴客戶及其「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「客戶支援入口網站」，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.ibm.com/software/security/trusteer/support）。

4. 計費

4.1 計費度量

本「雲端服務」之計費度量載明於「交易文件」中。

下列計費度量適用於本「雲端服務」：

- 「約定」為「雲端服務」有關專業或訓練服務。
- 「合格參與者」係為有資格參與本「雲端服務」所管理或追蹤之任何服務交付程式之「個人」或「實體」。
  - 「作用中使用者」係指透過任何方法以任何直接或間接方式（例如：透過多工程式、裝置或應用程式伺服器）存取「雲端服務」之特定使用者。
- 就 IBM Trusteer Pinpoint Detect Bundle 而言，「作用中使用者」係指於過去 12 個月之期間（於期間結束前）至少透過任何方式存取「雲端服務」一次之特定人員。
- 「應用程式」係為一種由「雲端服務」開發、提供存取權限或使用之特定指名軟體程式。
- 「API 呼叫」係為透過可程式介面呼叫「雲端服務」。
- 「連線」係指對先前或目前提供予「雲端服務」之資料庫、應用程式、伺服器或其他類型之裝置所為之鏈結或關聯。

4.2 遠端服務費用

遠端服務，不問已使用與否，悉於購買日起九十日後到期。

5. 附加條款

於 2019 年 1 月 1 日前簽署之「雲端服務合約」（或性質相當的基本雲端合約），適用 https://www.ibm.com/acs 所載明之條款。

5.1 資料當事人資料處理之 EULA 及依據

以下規定適用於 IBM Trusteer Rapport 雲端服務（如係連同 Pinpoint 雲端服務一併部署者，則包括 Rapport Remediation 或 Rapport for Mitigation）：除另有約定，並依 貴客戶獨立確認之前述處理依據，貴客戶授權 IBM 提供「終端使用者授權合約」（提供此合約之網址如下：https://trusteer.secure.force.com/PKB/articles/en_US/FAQ/RAPPORT-DATA-PRIVACY-NOTICE-AND-END-USER-LICENSE-AGREEMENT-EULA），使 IBM 得以蒐集及處理提供「雲端服務」所需之資訊。

貴客戶就 IBM Rapport Trusteer 雲端服務，授權 IBM 以「贊助企業」資料處理者之身分，利用本「程式」蒐集惡意軟體及惡意軟體構件（亦即，惡意活動相關檔案）或本「程式」異常故障相關檔案。IBM 不利用本「程式」將含有終端使用者個人資料之檔案當作鎖定目標；但所蒐集之檔案有可能內含未經終端使用者許可而自惡意軟體取得之個人資料。IBM 將遵循下列規定：1) 立即刪除與前揭分析無關之檔案；及 2) 僅於進行分析之期間保留該等相關檔案，在任何情形下，保留期間不得超過三個月。

5.2 其他處理位置資訊

「個人資料」之一切代管與處理（包括由 Data Sheet 所載明之第三方再處理者所為者）均應於以下所載位置為之：

對於透過德國資料中心提供之所有服務，IBM 會將「個人資料」之代管與處理限於 IBM 締約實體之國家/地區及下列國家/地區：德國、以色列、愛爾蘭及荷蘭。

對於透過日本資料中心提供之所有服務，IBM 會將「個人資料」之代管與處理限於 IBM 締約實體之國家/地區及下列國家/地區：日本、以色列及愛爾蘭。

對於透過美國資料中心提供之所有服務，IBM 會將「個人資料」之處理限於 IBM 締約實體之國家/地區及下列國家/地區：美國、以色列、愛爾蘭、新加坡及澳洲。

除前揭位置外，針對透過德國、日本及美國資料中心所提供之一切服務，(1) 另得由 Salesforce.Com 以 IBM 第三方再處理者之身分，於德國及法國代管及處理支援資料；及 (2) 若客戶選擇將資料傳送至 Mobile Carrier Intelligence 提供者，則得於 Data Sheet 所載適用第三方再處理者之國家/地區代管及處理「個人資料」。縱使 Data Sheet 有不同規定，前項第 (2) 款所載第三方再處理者仍可能未能符合 ISO 27001 或 SOC2 之規定。

IBM Trusteer 之支援與帳戶維護服務，亦得視需要，依據相關 IBM 人員可用度、 貴客戶位置及用以管理該等資料之資料中心提供之。

5.3 帳戶持有人資料

為求明確，茲進一步說明如下：特定「帳戶持有人」之「帳戶持有人用戶端軟體」有多個隸屬 IBM 客戶（該等 IBM 客戶以下稱為「隸屬客戶」），且本「服務說明」項下服務係由 IBM 透過位於不同區域之資料中心提供予該等「隸屬客戶」者，得於以上第 5.2 節所載各該資料中心有關一切位置處理該「帳戶持有人」之資料。

5.4 整合解決方案

為求明確，茲進一步說明如下：Trusteer 品牌旗下各種供應項目可能構成一個整合型解決方案。因此，倘若 貴客戶終止前揭各「雲端服務」之其中一項，IBM 為依據本「服務說明」提供 貴客戶其餘「雲端服務」，並依據其他 Trusteer 服務所適用之「服務說明」，提供 貴客戶其他 Trusteer 服務，得保留 貴客戶資料。

5.5 啟用軟體

本「雲端服務」內含下列「啟用軟體」：

- IBM Rapport Agents

5.6 Pinpoint 實作典範

若偵測到惡意軟體或帳戶接管， 貴客戶應遵循《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 Trusteer Pinpoint Detect 雲端服務，以免遭人利用 IBM Trusteer Pinpoint Detect 供應項目鏈結 貴客戶之動作（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）。

5.7 作為部署之一部分而蒐集之資料

貴客戶須提供 IBM 若干資料，始得部署本「雲端服務」。前述資料不得包含足以指明或歸屬特定個人之資訊。作為部署之一部分而提供予 IBM 之資料，其進一步準則檢附於擬提供予 貴客戶之「Trusteer 部署準則」。

6. 優先適用條款

6.1 資料之使用

雙方當事人所訂基本「雲端服務」條款之「內容及資料保護」一節有相反規定者，下列條款較該等規定優先適用：因 貴客戶使用本「雲端服務」所生結果，如為 貴客戶之「內容」（「洞察」）專屬結果或足資識別 貴客戶者，IBM 不予使用或揭露。但 IBM 為改善本「雲端服務」，得使用「內容」及其在提供本「雲端服務」時自「內容」（「洞察」除外）所產生之其他資訊。IBM 基於威脅偵測與保護之目的，亦得分享內嵌於「內容」之威脅識別碼及其他安全資訊。