# IBM Trusteer Fraud Protection

本「服務說明」敘述 IBM 提供予客戶之本「雲端服務」。「客戶」係指立約當事人、其授權使用者及本項「雲端服務」收受人。所適用之「報價單」及「權利證明書 (PoE)」係以個別「交易文件」之形式提供。

## 1. 雲端服務

本「服務說明」涵蓋下列「雲端服務」：

**Pinpoint Assure 雲端服務：**

- IBM Trusteer Pinpoint Assure
- IBM Trusteer Pinpoint Assure Application
- IBM Trusteer Mobile Carrier Intelligence

**Rapport「雲端服務」：**

- IBM Trusteer Rapport for Business Premium Support
- IBM Trusteer Rapport for Retail Premium Support
- IBM Trusteer Rapport II for Business
- IBM Trusteer Rapport II for Retail
- IBM Trusteer Rapport Fraud Feeds for Business
- IBM Trusteer Rapport Fraud Feeds for Business Premium Support
- IBM Trusteer Rapport Fraud Feeds for Retail
- IBM Trusteer Rapport Fraud Feeds for Retail Premium Support
- IBM Trusteer Rapport Phishing Protection for Business
- IBM Trusteer Rapport Phishing Protection for Business Premium Support
- IBM Trusteer Rapport Phishing Protection for Retail
- IBM Trusteer Rapport Phishing Protection for Retail Premium Support
- IBM Trusteer Rapport Mandatory Service for Business
- IBM Trusteer Rapport Mandatory Service for Retail
- IBM Trusteer Rapport Additional Applications for Retail
- IBM Trusteer Rapport Additional Applications for Business
- IBM Trusteer Rapport Large Redeployment
- IBM Trusteer Rapport Small Redeployment

**Pinpoint 雲端服務：**

- IBM Trusteer Pinpoint Malware Detection Standard Edition for Business Premium Support
- IBM Trusteer Pinpoint Malware Detection Standard Edition for Retail Premium Support
- IBM Trusteer Pinpoint Malware Detection Advanced Edition for Business Premium Support
- IBM Trusteer Pinpoint Malware Detection Advanced Edition for Retail Premium Support
- IBM Trusteer Rapport Remediation for Retail
- IBM Trusteer Rapport Remediation for Retail Premium Support
- IBM Trusteer Rapport Remediation for Business
- IBM Trusteer Rapport Remediation for Business Premium Support
- IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail
- IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business
- IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail

- IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business
- IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail
- IBM Trusteer Pinpoint Malware Detection Additional Applications for Business
- IBM Trusteer Pinpoint Malware Detection Redeployment
- IBM Trusteer Pinpoint Detect Standard for Retail
- IBM Trusteer Pinpoint Detect Premium for Retail
- IBM Trusteer Pinpoint Detect Standard for Business
- IBM Trusteer Pinpoint Detect Premium for Business
- IBM Trusteer Pinpoint Detect Standard Additional Applications for Business
- IBM Trusteer Pinpoint Detect Premium Additional Applications for Business
- IBM Trusteer Rapport for Mitigation for Retail
- IBM Trusteer Rapport for Mitigation for Retail Premium Support
- IBM Trusteer Rapport for Mitigation for Business
- IBM Trusteer Rapport for Mitigation for Business Premium Support
- IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail
- IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail
- IBM Trusteer Pinpoint Detect Standard Redeployment
- IBM Trusteer Pinpoint Detect Premium Redeployment
- IBM Trusteer Pinpoint Detect Standard for Retail Premium Support
- IBM Trusteer Digital Content Pack for Retail
- IBM Trusteer Digital Content Pack for Business
- IBM Trusteer New Account Fraud for Business
- IBM Trusteer New Account Fraud for Retail
- IBM Trusteer Project Management and Consultancy Services
- IBM Trusteer Security Research Consultancy Services
- IBM Trusteer Training Services
- IBM Trusteer Pinpoint Detect Standard Application
- IBM Trusteer Pinpoint Detect Premium Application
- IBM Trusteer Pinpoint Detect Standard
- IBM Trusteer Pinpoint Detect Premium
- IBM Trusteer Mobile Carrier Intelligence for Pinpoint Detect
- IBM Trusteer Pinpoint Verify

**Mobile 雲端服務：**

- IBM Trusteer Mobile SDK for Business
- IBM Trusteer Mobile SDK for Retail

## 1.1 商業與零售業雲端服務

IBM Trusteer「雲端服務」之授權係適用於搭配使用特定「應用程式」類型。所稱「應用程式」係定義為下列其中一種類型：「零售業」(Retail) 或「商業」(Business)。「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。

a. 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應用系統、行動式應用程式或電子商務應用程式。「客戶」之原則可將某些小型業務分類成適用於零售業存取。

b. 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。

### 1.1.1 商業雲端服務

- IBM Trusteer Rapport II for Business
- IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business
- IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business
- IBM Trusteer Pinpoint Detect Standard for Business
- IBM Trusteer Pinpoint Detect Premium for Business
- IBM Trusteer Digital Content Pack for Business
- IBM Trusteer New Account Fraud for Business
- IBM Trusteer Mobile SDK for Business

### 1.1.2 零售業雲端服務

- IBM Trusteer Rapport II for Retail
- IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail
- IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail
- IBM Trusteer Pinpoint Detect Standard for Retail
- IBM Trusteer Pinpoint Detect Premium for Retail
- IBM Trusteer Digital Content Pack for Retail
- IBM Trusteer New Account Fraud for Retail
- IBM Trusteer Mobile SDK for Retail

每一種「商業雲端服務」及「零售業雲端服務」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 Trusteer Mobile SDK「雲端服務」除外。

### 1.1.3 IBM Trusteer Rapport II 適用之額外「雲端服務」

a. IBM Trusteer Rapport for Business II 適用之額外「雲端服務」：
   - IBM Trusteer Rapport Fraud Feeds for Business
   - IBM Trusteer Rapport Phishing Protection for Business
   - IBM Trusteer Rapport Mandatory Service for Business
   - IBM Trusteer Rapport Additional Applications for Business

b. IBM Trusteer Rapport II for Retail 適用之額外「雲端服務」：
   - IBM Trusteer Rapport Fraud Feeds for Retail
   - IBM Trusteer Rapport Phishing Protection for Retail
   - IBM Trusteer Rapport Mandatory Service for Retail
   - IBM Trusteer Rapport Additional Applications For Retail

每一種 IBM Trusteer Rapport「雲端服務」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 Trusteer Rapport Mandatory Service 附加程式除外。

IBM Trusteer Rapport II for Business 或 IBM Trusteer Rapport II for Retail 之訂用係本節所列相關額外「雲端服務」之必備項目。

### 1.1.4 IBM Trusteer Pinpoint Malware Detection II 適用之額外「雲端服務」

a. IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business 或 IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business 適用之額外「雲端服務」：
   - IBM Trusteer Rapport Remediation for Business
   - IBM Trusteer Pinpoint Malware Detection Additional Applications for Business

b. IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail 或 IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail 適用之額外「雲端服務」：
   - IBM Trusteer Rapport Remediation for Retail

- IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail

頂級支援僅適用於本文件中規定之特定供應項目。IBM Trusteer Pinpoint Malware Detection II for Business 或 IBM Trusteer Pinpoint Malware Detection II for Retail 之訂用係本節所列相關額外「雲端服務」之必備項目。

**1.1.5 IBM Trusteer Pinpoint Detect Standard 及/或 IBM Trusteer Pinpoint Detect Premium 及/或 IBM Trusteer Pinpoint Detect Standard for Retail 及/或 IBM Trusteer Pinpoint Detect Premium for Retail 及/或 IBM Trusteer Pinpoint Detect Standard for Business 及/或 IBM Trusteer Pinpoint Detect Premium for Business 適用之額外「雲端服務」**

a. IBM Trusteer Detect Standard for Business 及/或 IBM Trusteer Pinpoint Detect Premium for Business 適用之額外「雲端服務」:
   - IBM Trusteer Pinpoint Detect Standard Additional Applications for Business
   - IBM Trusteer Pinpoint Detect Premium Additional Applications for Business
   - IBM Trusteer Digital Content Pack for Business
   - IBM Trusteer New Account Fraud for Business

b. IBM Trusteer Detect Standard for Retail 及/或 IBM Trusteer Pinpoint Detect Premium for Retail 適用之額外「雲端服務」:
   - IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail
   - IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail
   - IBM Trusteer Digital Content Pack for Retail
   - IBM Trusteer New Account Fraud for Retail

c. IBM Trusteer Pinpoint Detect Standard 及/或 IBM Trusteer Pinpoint Premium 適用之額外「雲端服務」:
   - IBM Trusteer Pinpoint Detect Standard Application
   - IBM Trusteer Pinpoint Detect Premium Application

d. IBM Trusteer Pinpoint Detect Premium 適用之額外「雲端服務」:
   - IBM Trusteer Pinpoint Verify

IBM Trusteer Pinpoint Detect Standard 或 IBM Trusteer Pinpoint Detect Premium 或 IBM Trusteer Pinpoint Detect Standard for Retail 或 IBM Trusteer Pinpoint Detect Premium for Retail 或 IBM Trusteer Pinpoint Detect Standard for Business 或 IBM Trusteer Pinpoint Detect Premium for Business 之訂用，係本節所列相關額外「雲端服務」之必備項目。

**1.1.6 其他額外「雲端服務」**

此處未列出前揭基本程式訂用所適用之額外「雲端服務」訂用，無論目前已提供或正在開發皆不被視為更新項目，故應另外取得其授權。

## 1.2 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「零售業應用程式」或「商業應用程式」（「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。

**"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 代管之網頁，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」。

## 1.3 IBM Trusteer Rapport「雲端服務」

### 1.3.1 IBM Trusteer Rapport II for Retail 及/或 IBM Trusteer Rapport II for Business ("Trusteer Rapport II")

Trusteer Rapport II 雲端服務為 IBM Trusteer Rapport 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。

Trusteer Rapport II 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」依「合格參與者」計費度量或「客戶裝置」計費度量之授權提供。本「商業」供應項目係以 10 位「合格參與者」或 10 個「客戶裝置」為一套組之方式銷售。本「零售」供應項目係以 100 位「合格參與者」或 100 個「客戶裝置」為一套組之方式銷售。

本項「雲端服務」供應項目包括：

a. Trusteer 管理應用程式 ("TMA")：

   TMA 係於 IBM Trusteer 雲端代管之環境中提供，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) 檢視並下載特定事件資料報告及風險評量；及 (ii) 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「客戶」之「合格參與者」，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：

   用於為存取或使用本「雲端服務」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」訂用本「雲端服務」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」進行至少一次鑑別後，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」訂用本「雲端服務」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」鑑別及行銷「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。客製啟動畫面得依另行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 所代管之登入頁面，以及 IBM 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原則。

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 Trusteer Rapport Mandatory Service 雲端服務。

「帳戶持有人用戶端軟體」之必要部署包括且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。

Trusteer Rapport II for Business 及/或 Trusteer Rapport II for Retail 各自包含一個「應用程式」之保護。「客戶」應就各額外「應用程式」取得 IBM Trusteer Rapport Additional Applications 之授權。

### 1.3.2 IBM Trusteer Rapport II for Business 及/或 IBM Trusteer Rapport II for Retail 適用之選用額外「雲端服務」

IBM Trusteer Rapport II 雲端服務之訂用，係為訂用下列任一額外「雲端服務」之必要條件。若該「雲端服務」載明為「商業使用」，則所取得之額外「雲端服務」亦需載明為「商業使用」。若該「雲端服務」載明為「零售業使用」，則所取得之額外「雲端服務」亦需載明為「零售業使用」。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」進行至少一次鑑別後，該等「合格參與者」或「客戶裝置」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。

### 1.3.3 IBM Trusteer Rapport Fraud Feeds for Business 及/或 IBM Trusteer Rapport Fraud Feeds for Retail

訂用本附加程式雲端服務後，「客戶」（及其不限數量之授權人員）可使用 TMA 檢視、訂用及配置從 Trusteer Rapport「雲端服務」所產生威脅資訊來源之遞送；資訊來源可由電子郵件傳送至指定電子郵件位址，或透過 SFTP 以文字檔之格式傳送。

本供應項目僅適用「合格參與者」計費度量。

### 1.3.4 IBM Trusteer Rapport Phishing Protection for Business 及/或 IBM 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騙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「雲端服務」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。

本「雲端服務」依「合格參與者」計費度量或「客戶裝置」計費度量之授權提供。本「商業」供應項目係以 10 位「合格參與者」或 10 個「客戶裝置」為一套組之方式銷售。本「零售」供應項目係以 100 位「合格參與者」或 100 個「客戶裝置」為一套組之方式銷售。

「客戶」得依「合格參與者」計費度量或「客戶裝置」計費度量取得本「雲端服務」之頂級支援。本「商業」供應項目係以 10 位「合格參與者」或 10 個「客戶裝置」為一套組之方式銷售。本「零售」供應項目係以 100 位「合格參與者」或 100 個「客戶裝置」為一套組之方式銷售。

### 1.3.5 IBM Trusteer Rapport Mandatory Service for Business 及/或 IBM 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」訂用本「雲端服務」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 Trusteer Rapport Premium Support for Business 係為 IBM Security Rapport Mandatory Service for Business 之必備項目。

IBM 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」訂用本「雲端服務」涵蓋項目後，須先訂購 IBM 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。

本「雲端服務」依「合格參與者」計費度量提供。本「商業」供應項目係以 10 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。

### 1.3.6 IBM Trusteer Rapport Large Redeployment 及/或 IBM Trusteer Rapport Small 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 Rapport II 部署之「客戶」，應購買 IBM Trusteer Rapport Redeployment 雲端服務。

「重新部署」有可能是因「客戶」變更「應用程式」之網域或主機 URL，而將變更套用至啟動畫面配置，或移至新線上銀行平台。

於 6 個月之重新部署轉移期間內，「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」。

IBM Trusteer Rapport Large Redeployment 適用於內含超過 20,000 位使用者之環境，IBM Trusteer Rapport Small Redeployment 則適用於內含至多 20,000 使用者之環境。

### 1.3.7 IBM Trusteer Rapport Additional Applications for Business 及/或 IBM Trusteer Rapport Additional Applications for Retail

必須取得 IBM Trusteer Rapport Additional Applications for Business 雲端服務之授權，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 Rapport II for Business。必須取得 IBM Trusteer Rapport Additional Applications for Retail 雲端服務之授權，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 Rapport II for Retail。

## 1.4 IBM Trusteer Pinpoint 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。「客戶」為「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. TMA：

TMA 係於 IBM Trusteer 雲端代管之環境中提供，透過此應用程式，「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。

b. Web Script 及/或 API：

用於為存取或使用本「雲端服務」而部署於網站。

### 1.4.1 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，「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「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）。

### 1.4.2 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「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，「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. 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。

**1.4.3 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。

**1.4.4 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「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。「客戶」應備有實際執行於「客戶」之「應用程式」之 IBM Trusteer Pinpoint Malware Detection II 之現行訂用。「客戶」僅限與存取「客戶」之「應用程式」之「合格參與者」一起使用本項「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「客戶」之「應用程式」進行至少一次鑑別，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「客戶」之一般「合格參與者」數量之權利。

**1.4.5 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「客戶」，應購買 IBM Trusteer Pinpoint Malware Detection Redeployment。

「重新部署」有可能是因「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，「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。

**1.4.6 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。

## 1.5 IBM Trusteer Fraud Protection Suite

IBM Trusteer Fraud Protection Suite ("Suite") 係為雲端型服務集合，此集合之設計目的在於提供防詐騙層，並可與其他 IBM 產品整合以提供生命週期管理解決方案。此 Suite 包括下列雲端型服務：

- IBM Trusteer Pinpoint Detect，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「雲端服務」涵蓋項目及防詐騙處理程序後，Trusteer Pinpoint Detect 便可整合至該等應用程式。
- IBM Trusteer Rapport for Mitigation，以重新修補及防護受感染端點為其目標。

「雲端服務」包括：

a. TMA：

TMA 係於 IBM Trusteer 雲端代管之環境中提供，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. 事件資料：

「客戶」為其「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，「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。

c. Web Script 及/或 API：

用於為存取或使用本「雲端服務」而部署於網站。

**Pinpoint 實作典範**

若偵測到惡意軟體或帳戶接管，「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 Trusteer Pinpoint Detect 雲端服務，以免遭人利用 IBM Trusteer Pinpoint Detect 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）。

### 1.5.1 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「客戶」（透過原生瀏覽器或「客戶」行動式應用程式）。

本項「雲端服務」包含標準支援（如以下「技術支援」一節所定義者）。如需「頂級」支援，「客戶」必須購買 Pinpoint Standard Premium Support。

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 Standard Additional Applications 之授權。

本項服務之購買，以「100 位合格參與者」或「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。

### 1.5.2 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「客戶」（透過原生瀏覽器或「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，「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「客戶」環境以調整「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，「客戶」必須遵循 IBM 準則進行規則設定，如說明文件中所約定。「客戶」確認，IBM 對於「客戶」未遵循建議而可能衍生之任何狀況概不負責。

任何因「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。

### 1.5.3 IBM Trusteer Pinpoint Detect Standard 及/或 IBM Trusteer Pinpoint Detect Premium 之選用服務

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

### 1.5.4 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「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。「客戶」應備有實際執行於「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。「客戶」僅限與存取「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「客戶」之「零售業應用程式」進行至少一次鑑別，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「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「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。「客戶」應備有實際執行於「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。「客戶」僅限與存取「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「客戶」之「商業應用程式」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「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。

### 1.5.5 IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail 及/或 IBM Trusteer Pinpoint Detect Standard Additional Applications for Business 及/或 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 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。
- 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。

### 1.5.6 IBM Trusteer Pinpoint Detect Standard Application 及/或 IBM Trusteer Pinpoint Detect Premium Application

本項服務適用於 Web 通道及「行動式」通道。

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 Standard ApplicationIBM Trusteer Pinpoint Detect Standard Application 之授權，始得部署 IBM Trusteer Pinpoint Detect Standard。
- 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。

### 1.5.7 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「客戶」，應購買 IBM Trusteer Pinpoint Detect Redeployment。

「重新部署」有可能是因「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，「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」。

### 1.5.8 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。

### 1.5.9 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、見解及政策，採購此等規則、見解及政策後，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。

### 1.5.10 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定功能蒐集之新活動，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。

### 1.5.11 IBM Trusteer Pinpoint Verify

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

本「雲端服務」具有對使用者進行第二個鑑別因素盤查之功能，俾為於其存取數位服務時驗證其身分。前述功能適用於 Pinpoint Detect Premium，俾以針對受保護應用程式提供第二個鑑別因素。有關何時就第二個鑑別因素對使用者進行盤查之決策，係由受保護應用程式產生，並以 Pinpoint Detect Premium 平台傳回之建議或受保護應用程式所訂其他政策為其依據。

## 1.6 IBM Trusteer Pinpoint Assure

本項服務可標示可疑活動，並於進行新帳戶建立/登錄程序時產生警示。本項服務會監測帳號登錄程序，以識別詐欺相關活動，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 Pinpoint Assure 係以 100 個「連線」為一套組之方式提供。

### 1.6.1 IBM Trusteer Pinpoint Assure 之選用服務

### 1.6.2 IBM Trusteer Pinpoint Assure Application

必須取得 IBM Trusteer Pinpoint Assure Application 之授權，始得於任一「應用程式」上部署 IBM Trusteer Pinpoint Assure。

IBM Trusteer Pinpoint Assure 係按應用程式購買之。

### 1.6.3 IBM Trusteer Mobile Carrier Intelligence 及/或 IBM Trusteer Mobile Carrier Intelligence for Pinpoint Detect

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

本項「雲端服務」藉由提供有關提供予 IBM Trusteer Pinpoint Assure 及/或 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「客戶」之內部用途，且僅限保留三十 (30) 日。逾前揭保留期限後，「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，「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」。

## 1.7 IBM Trusteer Remotely Delivered Services

IBM Trusteer Remotely Delivered Services 係以 Pinpoint Detect Premium 及 Pinpoint Assure 雲端服務之選用附加程式提供。

### 1.7.1 IBM Trusteer Project Management and Consultancy Services

本項服務提供二百小時之諮詢服務，在此期間 IBM 將執行下列部分或全部作業：

a. 起始設定服務：經常性定期會議、專案管理服務

b. Policy Manager：後續支援

本供應項目係按「約定」購買之。

### 1.7.2 IBM Trusteer Security Research Consultancy Services

本項諮詢服務最多包含 200 小時安全分析共用資源，其設計目的，在於提供所訂定之解決方案及頂級支援（在適用情形下）以外之額外服務，此等服務包括以下各項：

a. 延伸詐欺研究：每週會議與訓練。

b. 高優先順序「客戶」之發行版次支援

c. 後續客製規則調查及支援

本供應項目係按「約定」購買之。

### 1.7.3 IBM Trusteer Training Services

本項諮詢服務之設計，旨在提供所訂定之解決方案及頂級支援（在適用情形下）以外之額外服務，此等服務包括有關「客戶」受聘僱人員 Trusteer 投資組合之訓練服務。

本供應項目係按「約定」購買之。

## 1.8 IBM Trusteer Mobile 雲端服務

### 1.8.1 IBM Trusteer Mobile SDK for Business 及/或 IBM Trusteer Mobile SDK for Retail

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「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「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」））。

IBM Trusteer Mobile SDK for Retail 係以 100 個「合格參與者」或 100 個「客戶裝置」為一個套組之方式提供，IBM Trusteer Mobile SDK for Business 則以 10 個「合格參與者」或 10 個「客戶裝置」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，並可使「客戶」規劃防免詐騙之政策以對該等風險進行

控管行動。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 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，「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「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」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「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。

限於為支援其對「雲端服務」之使用，「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「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「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。

## 2. 內容及資料保護

Data Processing and Protection Data Sheet (Data Sheet) 提供有關為進行處理而啟用之「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之本項「雲端服務」特定資訊。有關本項「雲端服務」使用及資料保護特定功能之詳細內容或澄清及條款，包括「客戶」責任，於本節定之。依據「客戶」所選選項，「客戶」使用本項「雲端服務」時所適用之 Data Sheet 可能有一份以上。Data Sheet 可能僅以英文提供，不以當地語文提供。不問當地法律或慣例有任何之規定，雙方當事人同意其等皆瞭解英文，且英文為有關「雲端服務」之取得及使用之適當語文。下列 Data Sheet 適用於本項「雲端服務」及其可用選項。「客戶」確認 i) IBM 得自行決定隨時修改 Data Sheet，且 ii) 前述修改將取代

舊版本。以下各項為修改 Data Sheet 之目的：i) 改進或澄清現有承諾，ii) 與現行採用之標準及適用法令保持一致，或者 iii) 提供其他承諾。對 Data Sheet 之修改不會降低「雲端服務」之資料保護等級。

以下為適用 Data Sheet 之鏈結：

**IBM Trusteer Mobile SDK**

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

**IBM Trusteer Mobile Secure Browser**

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=1402492579396

**IBM Trusteer Pinpoint Assure**

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=CF0C527046E011E8ADCBA344DE8FB657

**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 Rapport**

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

**IBM Trusteer Pinpoint Verify**

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=735E5650E26711E69CCD7F0385C6524D

（IBM Cloud Identity Verify Data Sheet 會反映 IBM Trusteer Pinpoint Verify）

「客戶」有責任就「雲端服務」採取必要行動，以訂購、啟用或使用可用之資料保護特定功能，並接受其未能採取該等行動時所應承擔之有關使用「雲端服務」之責任，包括遵守有關「內容」之資料保護規定或其他法律之規定。

若歐盟一般資料保護規章 (EU/2016/679) (GDPR) 適用於「內容」所含個人資料，則於其適用的範圍內，IBM 之資料處理附錄 (DPA)（網址：http://ibm.com/dpa）及「DPA 附件」適用於本合約並為其補充。本項「雲端服務」所適用之 Data Sheet，應作為 DPA 附件。若適用於 DPA，則 IBM 對「再處理者」之變更通知義務，以及「客戶」得對該等變更提出異議之權利，依 DPA 之規定。

## 2.1 資料當事人資料處理之 EULA 及依據

**下列規定適用於 IBM Trusteer Rapport「雲端服務」（搭配 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「客戶」獨立確認之前述處理依據，「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://www.trusteer.com/support/end-user-license-agreement），使 IBM 得據以蒐集及處理為提供本「雲端服務」所需之資訊。

## 2.2 資料之使用

因「客戶」使用本項「雲端服務」所生結果，如為「客戶」之「內容」（「見解」）專屬結果或足資識別「客戶」者，IBM 不予使用或揭露。但 IBM 得使用「內容」及於提供本「雲端服務」時由「內容」所生其

他資訊（「見解」除外），惟需移除個人識別碼，俾以在不使用其他資訊之情形下，不再足以將該個人資料歸屬於特定個人。IBM 僅限於將該等資料使用於研究、測試及供應項目開發等用途。

## 2.3 資料之處理與儲存

### 2.3.1 其他處理位置資訊

Trusteer Pinpoint Verify 服務之所有主機作業及處理位置，均載明於相關 Data Sheet。

對於透過德國資料中心提供之其他所有服務，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：德國、以色列、愛爾蘭、荷蘭，以及「IBM 第三人再處理者」適用 Data Sheet 所列其他國家。

對於透過日本資料中心提供之其他所有服務，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：日本、以色列、愛爾蘭，以及「IBM 第三人再處理者」適用 Data Sheet 所列其他國家。

對於透過美國資料中心提供之其他所有服務，IBM 規定「個人資料」之處理應以 IBM 締約實體及下列國家/地區為限：美國、以色列、愛爾蘭、新加坡、澳洲，以及「IBM 第三人再處理者」適用 Data Sheet 所列其他國家/地區。

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

### 2.3.2 帳戶持有人資料

「帳戶持有人」資料之處理，應於「帳戶持有人」安裝「帳戶持有人用戶端軟體」之原區域為之。這表示，「帳戶持有人」內容之處理有可能同時於原區域及「客戶」所同意之區域為之。

### 2.3.3 整合解決方案

茲進一步釐清如下：因 Trusteer Fraud Protection 係為整合解決方案，倘若「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「客戶」其餘「雲端服務」，得保留「客戶」資料。

# 3. 服務水準協定

IBM 依「權利證明書」提供本「雲端服務」之可用度服務水準協定 ("SLA") 如下。本 SLA 並非保證。本 SLA 僅限提供予「客戶」，且僅適用於正式作業環境中之使用，

## 3.1 可用度扣抵

「客戶」應在得知事件影響「雲端服務」可用性之 24 小時內，先向 IBM 技術支援中心服務台記載「嚴重性層次 1」支援問題單。「客戶」應於合理範圍內協助 IBM 進行任何問題之診斷與解決。

就未能符合 SLA 而提出之支援問題單請求，應於合約月份結束後三個工作日內提出。對於有效 SLA 請求之補償，將以本項「雲端服務」未來發票扣抵方式提供之，該項扣抵之計算期間為無法提供本項「雲端服務」正式作業系統處理之期間（「停用時間」）。「停用時間」之計算，自「客戶」提報事件時起，至本項「雲端服務」回復時止，但不包括因下列事由所致時間：基於維修目的而排定或公布之停止；非 IBM 所能掌控之原因；因「客戶」或第三人內容或技術、設計或指示所生問題；不受支援之系統配置及平台或其他「客戶」錯誤；或「客戶」所致資安事故或「客戶」安全測試。IBM 將依各合約月份期間之本項「雲端服務」累計可用度，套用最高可適用之補償，如下表所示。 任何合約月份相關之補償總額，以本「雲端服務」年費十二分之一 (1/12) 的百分之十 (10%) 金額為上限。

## 3.2 服務水準

合約月份期間的本項「雲端服務」可用度

| 合約月份期間的可用度 | 補償<br>（請求事由發生之合約月份的每月訂用費用*之百分比） |
|---|---|
| <99.9% | 2% |
| < 99.0% | 5% |
| < 95.0% | 10% |

*如本項「雲端服務」係向「IBM 事業夥伴」取得者，每月訂用費用應以請求所主張之合約月份之有效本項「雲端服務」當時最新標價計算，且其折扣率為 50%。IBM 將直接折讓給「客戶」。

「服務水準」及相關「補償」扣抵依「雲端服務」及「客戶應用程式」個別計量。

以「應用程式」授權為依據之本「雲端服務」，於計算其 SLA 扣抵時，「可用度」之計算，依下列準則：

- 各「應用程式」依合約月份期間階段作業計數數目，各有其指定加權共用數量。
- 每一「應用程式」之各「雲端服務」，其停用時間於合約月份應個別累計。

下列範例計算一個月之活動及相關加權。僅供說明之用：

| 零售業應用程式 | 特定合約月份中階段作業總數之平均共用情況 | 合約月份期間總計停用時間 | 停用時間加權分鐘數 |
|---|---|---|---|
| 零售業應用程式 A | 40% | 300 分鐘 | 40% x 300 分鐘 = 120 分鐘 |
| 零售業應用程式 B | 20% | 250 分鐘 | 20% x 250 分鐘 = 50 分鐘 |
| 零售業應用程式 C | 40% | 150 分鐘 | 40% x 150 分鐘 = 60 分鐘 |
| | | | 停用時間之總加權分鐘數 = 230 分鐘 |

可用度（以百分比表示）之計算為：合約月份中的總分鐘數減去合約月份中「停用時間」之總加權分鐘數，除以合約月份之總分鐘數。以下為依據上列加權範例所為計算範例：

30 天「合約月份」，總共 43,200 分鐘
- 230 分鐘之加權停用時間
= 42,970 分鐘

總共 43,200 分鐘

= 合約月份期間可用度達 99.4% 時為 2% 可用度扣抵

## 4. 技術支援

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

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「雲端服務」頂級支援訂用，須另外收取費用，但 **IBM Trusteer Mobile SDK 雲端服務**及 **IBM Trusteer Rapport Mandatory Service 雲端服務**、**IBM Trusteer New Account Fraud**、**IBM Trusteer Pinpoint Assure**、**IBM Trusteer Digital Content Pack** 及 **IBM Trusteer Mobile Carrier Intelligence** 除外。請聯絡 IBM 業務代表或 IBM 事業夥伴。

**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 IBM 軟體即服務 (SaaS) 手冊，此手冊提供於下列網站：https://www.ibm.com/software/support/saas_support_guide.html。
- 「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-01.ibm.com/software/security/trusteer）。

**頂級支援：**

- 為所有嚴重性的問題提供全年無休支援。
- 「客戶」可直接透過電話及回電申請取得支援。
- 「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「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）。

- 如需支援選項及詳細資料相關資訊，請存取 IBM 軟體即服務 (SaaS) 手冊，此手冊提供於下列網站：https://www.ibm.com/software/support/saas_support_guide.html。

## 5. 授權與付款資訊

### 5.1 計費度量

本項「雲端服務」係依「交易文件」中所定計費度量而提供。

- 「約定」(Engagement) 是取得服務所需的一種計量單位。一個「約定」(Engagement) 係由有關本「雲端服務」的專業及/或訓練服務組成。「客戶」應取得足夠的授權數，以涵蓋每一個「約定」。
- 「合格參與者」(Eligible Participant) 是取得本項「雲端服務」所需的一種計量單位。 個人或實體，取得由本「雲端服務」管理或追蹤之任何服務交付程式之參與資格者，即為「合格參與者」。「客戶」應取得足夠涵蓋在其「交易文件」中所指定計量期間於「雲端服務」內管理或追蹤之所有「合格參與者」的授權數。

  由本「雲端服務」管理之每一項服務交付程式，均先予以個別分析後再合併。符合多重服務交付程式資格之個人或實體，需另行取得獨立授權。

  基於前述「雲端服務」之授權目的，「合格參與者」係指「客戶」之「終端使用者」，該使用者備有「客戶」之「商業應用程式」或「零售業應用程式」之唯一登入認證。
- 「客戶裝置」是取得本「雲端服務」所需的一種計量單位。「客戶裝置」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。多個客戶裝置可使用同一部共用伺服器。客戶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。「客戶」應為在「客戶」的「交易文件」中所指定之計量期間、執行本「雲端服務」、提供資料給本「雲端服務」、使用由本項「雲端服務」提供的服務，或以其他方式存取本「雲端服務」之每一個「客戶裝置」取得授權。
- 「應用程式」是取得本「雲端服務」所需的一種計量單位。「應用程式」係為一種唯一指名軟體程式。「客戶」應取得足夠讓在其「權利證明書 (PoE)」或「交易文件」中所指定計量期間之每一「應用程式」可供存取及使用的授權。

  基於本「雲端服務」之目的，「應用程式」係指「客戶」之單一「商業應用程式」或「零售業應用程式」。
- 「API 呼叫」是取得本項「雲端服務」所需的一種計量單位。「API 呼叫」係為透過可程式介面呼叫本項「雲端服務」。「客戶」應取得足夠涵蓋在其「權利證明書」或「交易文件」中所指定計量期間之「API 呼叫」總數之授權，該總數無條件進位至最接近之十位數。
- 「連線」是取得本「雲端服務」所需的一種計量單位。一個「連線」是指資料庫、應用程式、伺服器或任何其他類型之裝置與「雲端服務」的一個鏈結或關聯。「客戶」應取得足夠涵蓋在其「權利證明書」或「交易文件」中所指定計量期間已對或將對「雲端服務」建立的「連線」總數的授權數。

  基於本「雲端服務」之目的，「連線」係指「客戶」之「應用程式」中之階段作業或流程。

### 5.2 超額使用計費

若「客戶」在計量期間內的本項「雲端服務」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於超額使用後之翌月，依「交易文件」所定費率計費。

### 5.3 計費頻率

IBM 將於計費頻率期間起算日，依選定計費頻率對「客戶」開立應付款項之發票，惟超額使用款項及應以後付方式開立發票之使用類型款項除外。

## 6. 期間及續約選項

本項「雲端服務」之期間，自 IBM 通知「客戶」其可存取本「雲端服務」之當日起算，詳如「權利證明書」上所載。權利證明書將載明本「雲端服務」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」於前述期間到期日九十日（或更早）前為不續約之書面通知，否則，本項「雲端服務」將依「權利證明書」所載明之期間自動續約。續約時可能調升年度價格，如報價單所示。如係於收到 IBM 為撤銷本項「雲端服務」之通知後自動續約者，續約期間之終止日為現行續約期間結束日或所公布之撤銷日期（以發生在先者為準）。

如係持續使用，將依按月之方式持續提供本項「雲端服務」，至「客戶」提供九十日前終止之書面通知為止。於前述到期日九十日前之期間後至該日曆月月底前，將繼續提供本項「雲端服務」。

## 7. 其他條款

### 7.1 一般規定

「客戶」同意 IBM 得於宣傳或行銷傳播時公開稱「客戶」為本「雲端服務」之訂用者。

「客戶」不得為支援下列高風險活動而使用「雲端服務」，不論係單獨使用或結合其他服務或產品一併使用，均同：核能機構、大眾運輸系統、空中交通管制系統、汽車控制系統、武器系統或飛航導航或通訊系統之設計、建構、控制或維護，或其他因本「雲端服務」失效而可能引起重大傷亡危害之任何活動。

### 7.2 啟用軟體

本項「雲端服務」必須使用「客戶」下載至「客戶」系統之啟用軟體，以協助使用本項「雲端服務」。「客戶」僅限搭配本項「雲端服務」一併使用啟用軟體。啟用軟體依「現狀」提供。

### 7.3 IBM Trusteer Fraud Protection 之部署

就「客戶」所訂用之每一「應用程式」，「客戶」之基本程式訂用包含 IBM Trusteer 雲端上之必要設定及起始部署活動，包括起始一次啟動、配置、「啟動畫面範本」、測試及訓練。

部署活動不包括「客戶」之「應用程式」或系統所需之實作活動。

各種「雲端服務」之實作階段，係設計為於相關部署手冊所詳述之時間範圍內實作。

是否能於所分配之時間範圍內完成前項實作階段，取決於「客戶」之管理階層及人員能否全力支持及參與。「客戶」應及時提供所需資訊。IBM 之效能取決於「客戶」之及時資訊與決策，任何延遲均可能導致額外成本及/或延遲完成這些實作服務。

就「客戶」所訂用之每一「應用程式」，「客戶」之基本程式訂用包含 IBM Trusteer 雲端上之必要設定及起始部署活動，包括起始一次啟動、配置、「啟動畫面範本」、測試及訓練。

「客戶」之訂用包含特定頁面之支援與測試，所稱特定頁面，係指由 IBM 於起始部署時標示為建議使用之「客戶」應用程式所含頁面。IBM 對下列事項概不負責：(i) 局部部署；(ii)「客戶」選擇不依 IBM 所建議之方式部署 IBM 雲端服務；或 (iii)「客戶」選擇自行執行部署、設定及測試。(IV) 因「客戶」所提供之不適當資訊所致局部部署或保護。額外服務（包括起始部署以外之部署活動）需依另行簽立合約並收取額外費用後而提供。