

IBM Trusteer Pinpoint Assure

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 Assure 為依用途建置之高安全性分層解決方案，有助於防範有詐欺意圖之個人使用遭竊身分、新增假資料至真身分，或建立假造身分，進而利用該等身分，代表現有客戶進行來賓交易、開立全新帳戶或開立新數位帳戶。

1.1 供應項目

1.1.1 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「Trusteer 管理應用程式」(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驟帳戶或可能用於進行詐欺活動。IBM Trusteer Pinpoint Detect 及 IBM Trusteer Pinpoint Verify 係作為 TMA 登入之一部分。

IBM Trusteer Pinpoint Assure 係以每年 100 個「連線」為一套組之方式提供。

1.2 選用服務

1.2.1 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。

1.2.2 IBM Trusteer Mobile Carrier Intelligence

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

本「雲端服務」藉由提供有關提供予前揭各「雲端服務」之其中一項之行動電話號碼之額外資訊及環境定義，加強 IBM Trusteer Pinpoint Assure，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」。

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 5.1 節（「其他處理位置資訊」）。

IBM Trusteer Assure

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

IBM Trusteer Mobile SDK

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

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）。

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」：

- 「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。
- 「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。

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 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。

5.2 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。

5.3 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。