

IBM Trusteer Mobile

本「サービス記述書」は「クラウド・サービス」について規定するものです。該当する注文関連文書には、お客様の発注に関する価格の詳細情報および追加の詳細情報が記載されています。

1. クラウド・サービス

IBM Trusteer Mobile は、デバイスおよびセッションのリアルタイムのリスク検出を支援します。高度な分析およびリアルタイムのデバイス・リスク検出の活用により、組み込み先のアプリケーションの整合性を維持できます。Trusteer Mobile はデバイスを評価し、マルウェア、リモート・アクセス型トロイの木馬、脱獄 (jailbroken)/root 化の検出、オーバーレイ攻撃のエビデンス、および SMS 窃盗アプリケーションなどのセキュリティ侵害を受けているかどうかを判別します。行動異常、ナビゲーション不一致、フィッシングのセキュリティ侵害など、高度なテクノロジーを活用してその他のクロスチャネルの指標が継続的に処理されます。

1.1 オファリング

お客様は、利用可能な以下のオファリングから選択することができます。

1.1.1 IBM Trusteer Mobile SDK for Business および IBM Trusteer Mobile SDK for Retail

IBM Trusteer Mobile SDK の「クラウド・サービス」は、お客様が申し込んでいる「クラウド・サービス」の範囲、デバイスのリスク評価、およびファームウェアからの保護の対象である、お客様の「法人向けアプリケーション」および「個人向けアプリケーション」(またはそのいずれか) への安全な Web アクセスを提供する、別の保護層を追加できるように設計されています。セキュアな Wi-Fi 検出は、Android プラットフォームに関してのみ利用可能です。

IBM Trusteer Mobile SDK の「クラウド・サービス」には、文書、専有のプログラミング・ソフトウェア・ライブラリー、および関連するその他のファイルや品目 (IBM Trusteer モバイル・ライブラリーおよび「ランタイム・コンポーネント」と呼ばれます。) を含んだソフトウェア・パッケージである専有のモバイル・ソフトウェア開発者キット (以下「SDK」といいます。)、または、お客様が申し込んでいる「クラウド・サービス」の範囲の対象である、お客様の保護されたスタンドアロンの iOS または Android のモバイル・アプリケーションに組み込んだり、統合したりできる IBM Trusteer Mobile SDK (以下「お客様統合モバイル・アプリ」といいます。) で生成される専有コードである「再配布可能コード」が含まれます。

IBM Trusteer Mobile SDK for Retail は、「適格参加者」100 人単位または「クライアント・デバイス」100 個単位のパックで入手可能です。また IBM Trusteer Mobile SDK for Business は、「適格参加者」10 人単位または「クライアント・デバイス」10 個単位のパックで入手可能です。

TMA により、お客様 (および無制限数のお客様の有資格担当者) はイベント・データ・レポートおよびリスク・トレンド・アセスメントを受け取ることができます。IBM Trusteer Pinpoint Detect および IBM Trusteer Pinpoint Verify は、TMA ログインの一部として使用されます。「お客様統合モバイル・アプリ」により、お客様は、「お客様統合モバイル・アプリ」のダウンロード先である「適格参加者」のモバイル・デバイスに関連するリスク分析およびデバイス情報を受け取ることができます。これによりお客様は、これらのリスクに対する低減措置を実施する不正行為防止ポリシーを構築することができます。このオファリングの場合、「モバイル・デバイス」にはサポート対象のスマートフォンまたはタブレットのみが含まれ、PC および MAC は含まれません。

お客様は、以下を行うことができます。

- a. 「お客様統合モバイル・アプリ」の開発のみを目的として、社内で IBM Trusteer Mobile SDK を使用すること。
- b. 必須の分離不可能な方法として「再配布可能コード」を「お客様統合モバイル・アプリ」に組み込むこと (オブジェクト・コード形式のみによる)。この使用許諾に基づき修正またはマージされた「再配布可能コード」の部分には、本「サービス記述書」の条件が適用されるものとします。

- c. 「適格参加者」のモバイル・デバイス上または「クライアント・デバイス」ホルダー上にダウンロードするために「再配布可能コード」を促進して配布すること。ただし、以下を条件とします。
- 「本契約」で明示的に許可されている場合を除き、お客様は以下を行うことができません。
(1) SDK を使用、コピー、修正、配布すること、(2) 強制定規に別段の定めのある場合を除き、SDK を逆アセンブル、逆コンパイル、その他翻案、およびリバース・エンジニアリングすること、(3) SDK を再使用許諾、賃貸、リースすること、(4) 「再配布可能コード」に含まれる著作権や特記事項のファイルを削除すること、(5) 元の「再配布可能コード」のファイルやモジュールと同じパス名を使用すること、および(6) IBM または IBM のライセンサーもしくはディストリビューターの書面による事前同意なしで、IBM、IBM のライセンサーまたはディストリビューターの名称もしくは商標を「お客様統合モバイル・アプリ」のマーケティングに関連して使用すること。
 - 「再配布可能コード」は、「お客様統合モバイル・アプリ」内で切り離し不可能な方法で統合され続ける必要があります。「再配布可能コード」は、オブジェクト・コード形式のみである必要があります。また、SDK およびその文書に関するすべての指示、命令および仕様を満たす必要があります。「お客様統合モバイル・アプリ」のエンド・ユーザーのご使用条件には、「再配布可能コード」が、i) 「お客様統合モバイル・アプリ」の有効化以外の目的で使用できないこと、ii) コピーできないこと(バックアップ目的の場合を除く)、iii) さらに配布したり、転送したりできないこと、およびiv) 法律で明確に許可されている場合や契約で権利放棄することができない場合を除き、逆アセンブル、逆コンパイル、その他の方法により翻案できないことを、エンド・ユーザーに通知する必要があります。お客様のご使用条件は、少なくとも本契約の条件と同程度に IBM を保護するものである必要があります。
 - SDK は、お客様の指定モバイル・テスト・デバイスに関する、お客様の内部開発および単体テストの一部としてのみ展開できます。お客様には、実動ワークロードを処理したり、実動ワークロードのシミュレーションを行ったり、コード、アプリケーション、システムの拡張容易性をテストしたりすることはできません。お客様は、SDK のいかなる部分もその他の目的で利用することはできません。

お客様は、「お客様統合モバイル・アプリ」の開発、テストおよびサポートについて全責任を負います。お客様は、「お客様統合モバイル・アプリ」に対するあらゆる技術支援に対して、および本書で認められているとおりの「再配布可能コード」に対する変更に対して責任を負うものとします。

お客様は、お客様による「クラウド・オフライン」の使用をサポートするためにのみ、「再配布可能コード」および IBM Security Mobile SDK をインストールして使用する権限を付与されます。

IBM は、IBM Security Mobile SDK に含まれるモバイル・ツールを使用して作成されたアプリケーションまたはアウトプットが、特定のモバイル・オペレーティング・システム・プラットフォームもしくはモバイル・デバイスで機能すること、それらと相互運用すること、それらと互換性があることを保証しません。

「ソース・コンポーネント」および「サンプル資料」 - IBM Trusteer Mobile SDK には、ソース・コード・フォームの一部コンポーネント(以下「ソース・コンポーネント」といいます。)および「サンプル資料」に指定されるその他の資料が含まれる場合があります。お客様は、「ソース・コンポーネント」および「サンプル資料」の使用が「本契約」の下での許諾権制限の範囲内にある限り、お客様の内部使用を目的としてのみコピーおよび変更することができます。ただし、お客様は「ソース・コンポーネント」および「サンプル資料」に含まれる著作権情報または表示を変更または削除しないものとします。IBM は、「ソース・コンポーネント」および「サンプル資料」を、サポート義務を負わずに現状の状態で提供します。「ソース・コンポーネント」または「サンプル資料」が CIMA に「埋め込み可能なもの」を実装する方法の例としてのみ提供されていること、「ソース・コンポーネント」および「サンプル資料」にお客様の開発環境との互換性を持たせてはならないこと、ならびにお客様は CIMA に「埋め込み可能なもの」のテストおよび実装について全責任を負うことにご留意ください。

2. データ処理およびデータ保護に関するデータ・シート

IBM のデータ処理補足契約書 (<http://ibm.com/dpa>) に公開。「DPA」のほか、以下のリンクの「データ処理およびデータ保護に関するデータ・シート」(データ・シートまたは「DPA 別表」)にも、「クラウ

ド・サービス」およびそのオプション(処理対象の「コンテンツ」の種類、対象となる処理活動、データ保護機能、および「コンテンツ」の保存および返却についての仕様に関連)に関する追加的なデータ保護情報が記載されています。DPAは、i) EU一般データ保護規則(EU/2016/679)(GDPR)、またはii) <http://ibm.com/dpa/dpl>に記載されているその他のデータ保護法が適用される場合に、その適用範囲に限り、「コンテンツ」に含まれる個人データに適用されます。

「データ・シート」には通常、サービスの実施元であるデータセンターに関わりなく、IBM(第三者の復処理者が含まれます。)が「個人データ」をホストおよび処理するすべてのロケーションが列記されています。サービスの実施元であるデータセンターに固有の、ホスティング・ロケーションおよび処理ロケーションを記載したリストについては、後述の第5.1項(処理ロケーションに関する追加情報)を参照してください。

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>

3. サービス・レベルおよびテクニカル・サポート

3.1 サービス・レベル・アグリーメント

IBMは、以下の可用性のサービス・レベル・アグリーメント(以下「SLA」といいます。)をお客様に提供します。IBMは、下表のとおり、「クラウド・サービス」の累積的な可用性に基づき、適用しうる最大の補償を適用します。「可用性」は、契約月における分単位の総時間数から、契約月における「サービス・ダウン」の分単位の総時間数を差し引き、それを契約月における分単位の総時間数で除することにより算出され、結果はパーセントで表します。「サービス・ダウン」の定義、請求のプロセス、サービスの可用性の問題に関してIBMに連絡する方法については、IBMの「クラウド・サービス」のサポート・ハンドブック(https://www.ibm.com/software/support/saas_support_overview.html)に掲載されています。

可用性	クレジット (月額サブスクリプション料金のパーセント*)
99.9% 未満	2%
99.0% 未満	5%
95.0% 未満	10%

*サブスクリプション料金は、請求対象月に関して約定した料金です。

3.2 テクニカル・サポート

「クラウド・サービス」のテクニカル・サポート(サポート窓口の連絡先情報、重大度レベル、サポート利用可能時間、応答時間、その他のサポート情報およびサポート・プロセスなど)を参照するには、IBMサポート・ガイド(<https://www.ibm.com/support/home/pages/support-guide/>)の「クラウド・サービス」を選択します。

4. 料金

4.1 課金単位

「クラウド・サービス」の課金単位は、「個別契約書」に記載されます。

以下の課金単位が本「クラウド・サービス」に適用されます。

- 「適格参加者」とは、「クラウド・サービス」が管理または追跡するサービス提供プログラムに参加できる個人または法人です。

- 「クライアント・デバイス」とは、「クラウド・サービス」へアクセスするサーバー環境から、実行コマンド、手続き、またはアプリケーションを要求または受信するデバイスのことです。

5. 追加条件

2019年1月1日よりも前に締結されるクラウド・サービス契約書(または同等のクラウド基本契約)については、<https://www.ibm.com/acs>に掲載されている条件を適用します。

5.1 処理ロケーションに関する追加情報

「個人情報」のすべてのホスティングおよび処理(「データ・シート」に記載されている第三者の復処理者による場合を含みます。)は、下記のロケーションで実施されます。

ドイツのデータセンターを通じて提供されるすべてのサービスに関して、IBMは、「個人データ」のホスティングおよび処理を、IBMが契約を結んでいる事業体の所在国および以下の各国に限定するものとします。ドイツ、イスラエル、アイルランド、オランダ。

日本のデータセンターを通じて提供されるすべてのサービスに関して、IBMは、「個人データ」のホスティングおよび処理を、IBMが契約を結んでいる事業体の所在国および以下の各国に限定するものとします。日本、イスラエル、アイルランド。

米国のデータセンターを通じて提供されるすべてのサービスに関して、IBMは、「個人データ」のホスティングおよび処理を、IBMが契約を結んでいる事業体の所在国および以下の各国に限定するものとします。米国、イスラエル、アイルランド、シンガポール、オーストラリア。

上記のロケーションに加えて、ドイツ、日本、および米国のデータセンターを通じて提供されるすべてのサービスに関して、関連データが、IBMの第三者復処理者としてのSalesforce.Comによりドイツおよびフランスでホストまたは処理される場合があります。

IBM Trusteerに関するサポートおよびアカウント保守のサービスは、関連するIBM要員の対応時間の有無、お客様の所在地、およびデータがホストされているデータセンターに基づき、必要に応じて提供される場合もあります。

5.2 統合ソリューション

明確にするために付言すると、Trusteerブランドの各種オファリングは統合ソリューションを構成している場合があります。そのため、お客様が該当する「クラウド・サービス」のいずれかを終了した場合、IBMは、本「サービス記述書」に基づいて残りの「クラウド・サービス」を、およびその他のTrusteerサービスに適用されるサービス記述書に従って当該Trusteerサービスをお客様に提供する目的で、お客様のデータを保管することができます。

5.3 確認

お客様は、i) IBM およびその独立監査人がお客様の本契約の遵守状況を確認するために合理的に必要な記録、システム・ツールの出力を保管し、要求に応じて提供するものとします。また、ii) かかる確認の結果必要と判断された使用許諾を、IBMのその時点における最新の料金ですみやかに注文して支払うほか、その他の料金および債務を、IBMの請求書の記載に従い支払うものとします。これらの遵守状況の確認義務は、該当する「クラウド・サービス」の有効期間中および期間後の2年間有効に存続します。

5.4 導入の一部として収集されたデータ

「クラウド・サービス」の導入には、お客様からIBMへの特定のデータの提供を伴う場合があります。導入の一部としてお客様からIBMへ提供されるデータのガイドラインは、お客様に提供される「Trusteer導入ガイドライン」に記載されています。

6. オーバーライド条件

6.1 データの利用

両当事者間の「クラウド・サービス」基本条件の「コンテンツおよびデータ保護」項にいかなる矛盾する規定があっても、以下の条件が優先します。IBMは、お客様の「クラウド・サービス」の利用によって生まれるお客様の「コンテンツ」に固有のものである結果(以下「洞察」といいます。)や、お客様を特定できる結果を利用したり開示したりしません。ただし、IBMは、個人を特定する情報を削除し、追加情報を用いなければいかなる個人情報も特定の個人に結びつけることができないようにしたうえで、「クラウド・サービス」の一環として、「コンテンツ」および「コンテンツ」に由来するその他の情報を使用します。IBMは、研究、テスト、およびオフライン開発の目的でのみ、このデータを使用します。