IBM Trusteer Rapport

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 Rapport は、マルウェアやフィッシング攻撃からユーザーを保護するように設計された先進的なエンドポイント保護ソリューションです。

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 Rapport for Retail および IBM Trusteer Rapport for Business (以下「Trusteer Rapport」といいます。)

「Trusteer Rapport」は、フィッシングおよび MITB (マン・イン・ザ・ブラウザー) マルウェア攻撃に対する保護層を提供します。IBM Trusteer Rapport は世界中の数千万ものエンドポイントからなるネットワークを活用して、組織・団体を対象に世界規模で活発に行われているフィッシング攻撃やマルウェア攻撃の情報を収集します。IBM Trusteer Rapport は、フィッシング攻撃の防止とさまざまな MITB マルウェアのインストールや実行の防止を目的とする行動アルゴリズムを適用します。

本「クラウド・サービス」では、「適格参加者」の課金単位が設定されています。「法人向け」オファリングは、「適格参加者」10 人単位のパックで販売されています。「個人向け」オファリングは、「適格参加者」100 人単位のパックで販売されています。

本「クラウド・サービス」オファリングには以下が含まれます。

a. Trusteer Management Application (以下「TMA」といいます。)

TMA は、IBM Trusteer のクラウド・ホスティング環境で利用できるようになっており、お客様 (および人数の制限なく有資格担当者) は TMA により、(i) 特定のイベント・データ報告およびリスク評価を表示してダウンロードすること、ならびに (ii)「アカウント・ホルダーのクライアント・ソフトウェア」(以下に定義) の構成を表示することができます。お客様は、Trusteer Splash または Rapport API を使用する「アカウント・ホルダーのクライアント・ソフトウェア」のみを促進することができます。お客様は、社内業務の実行またはその従業員による使用 (従業員による個人的使用を除きます) のために「アカウント・ホルダーのクライアント・ソフトウェア」を利用することはできません。本「サービス記述書」において、「アカウント・ホルダー」とは、お客様のエンド・ユーザーのうち、クライアント・イネーブリング・ソフトウェアをインストール済みで、ソフトウェア使用許諾契約 (以下「EULA」といいます。) を受諾しており、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「個人向けアプリケーション」または「法人向けアプリケーション」で少なくとも 1 回は認証を受けているエンド・ユーザーをいいます。「アカウント・ホルダーのクライアント・ソフトウェア」とは、IBM Trusteer Rapport のクライアント・イネーブリング・ソフトウェア、または、エンド・ユーザーのデバイスにインストールするために一部の「クラウド・サービス」と共に提供されるその他のクライアント・イネーブリング・ソフトウェアをいいます。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。IBM は、お客様のエンド・ユーザーが「クラウド・サービス」の一部として提供されている「アカウント・ホルダーのクライアント・ソフトウェア」を適切にダウンロードしてインストールできるようにするために、IBM のオンライン・サポート・ポータルでお客様を公に特定する場合があります。

b. Web スクリプト

「クラウド・サービス」にアクセスするため、またはそれをテストもしくは使用するための、Web サイトでのアクセス用です。

c. イベント・データ

お客様 (および人数の制限なくお客様の有資格担当者) 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「法人向けアプリケーション」または「個人向けアプリケーション」と「アカウント・ホルダー」との間のオンライン対話の結果として「アカウント・ホルダーのクライアント・ソフトウェア」から生成されたイベント・データを受け取るために、TMA を使用することができます。イベント・データは、EULA を受諾し、お客様の「法人向けアプリケーション」または「個人向けアプリケーション」で少なくとも 1 回は認証を受けている「適格参加者」の「アカウント・ホルダーのクライアント・ソフトウェア」(それぞれのデバイス上で実行中のもの) から受け取ります。また、お客様の構成には、ユーザー ID の収集を含める必要があります。

d. Trusteer Splash

Trusteer Splash マーケティング・プラットフォームでは、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「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) にアクセスする「適格参加者」が特定され、当該「適格参加者」に「アカウント・ホルダーのクライアント・ソフトウェア」が促進されます。お客様は、利用可能な「Splash テンプレート」から選択することができます。カスタマイズされたスプラッシュを、別途合意書または作業指示書に基づいて契約することができます。

お客様は、TMA、Trusteer Splash と関連して用いるために、および「アカウント・ホルダーのクライアント・ソフトウェア」内、またはお客様のために IBM によりホストされるランディング・ページ上で表示するために、自社の商標、ロゴ、またはアイコンを提供することを選択できます。IBM は、お客様が指定する文脈においてのみ、商標、ロゴ、またはアイコンを使用するものとします。

お客様が「アカウント・ホルダーのクライアント・ソフトウェア」についてあらゆるタイプの強制導入を採用することを希望する場合、お客様は IBM Trusteer Rapport Mandatory Service の「クラウド・サービス」を申し込む必要があります。

「アカウント・ホルダーのクライアント・ソフトウェア」の強制導入には、以下が含まれますが、これらに限定されません。「適格参加者」に「アカウント・ホルダーのクライアント・ソフトウェア」のダウンロードを直接的または間接的に強制するメカニズムもしくは手段、または、「アカウント・ホルダーのクライアント・ソフトウェア」のこの強制導入に関する使用許諾の要件を免れるために作成された、IBM が作成したり、承認したりしたものではない、あらゆる方法、ツール、手順、合意、またはメカニズムを用いたあらゆるタイプの強制導入。

1.2 オプション・サービス

IBM Trusteer Rapport の追加のクラウド・サービス

a. IBM Trusteer Rapport II for Business に対して利用可能な追加のクラウド・サービス

- 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 に対して利用可能な追加のクラウド・サービス

- 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

IBM Trusteer Rapport の「クラウド・サービス」に対する「法人向け」および「個人向け」のアドオンごとに、追加料金で提供される、関連プレミアム・サポート製品があります。ただし、IBM Trusteer Rapport Mandatory Service アドオンは除きます。

IBM Trusteer Rapport II for Business または IBM Trusteer Rapport II for Retail のサブスクリプションは、本項に記載の関連する追加の「クラウド・サービス」の前提条件です。

1.2.1 IBM Trusteer Rapport II for Business および IBM Trusteer Rapport II for Retail に対するオプションの追加のクラウド・サービス

IBM Trusteer Rapport II Cloud Services のサブスクリプションは、以下の追加の「クラウド・サービス」のサブスクリプションの前提条件です。「クラウド・サービス」に「法人向け」の指定がある場合は、取得された追加の「クラウド・サービス」も「法人向け」と指定する必要があります。「クラウド・サービス」に「個人向け」の指定がある場合は、取得された追加の「クラウド・サービス」も「個人向け」と指定する必要があります。お客様は、EULA を受諾し、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) で少なくとも 1 回は認証を受けている「適格参加者」または「クライアント・デバイス」(「アカウント・ホルダーのクライアント・ソフトウェア」の実行者) からイベント・データを受け取ります。また、お客様の構成には、ユーザー ID の収集を含める必要があります。

1.2.2 IBM Trusteer Rapport Fraud Feeds for Business および IBM Trusteer Rapport Fraud Feeds for Retail

このアドオンの「クラウド・サービス」を申し込む際、お客様 (および人数の制限なくお客様の有資格担当者) は、Trusteer Rapport の「クラウド・サービス」から生成された脅威フィードの提供を表示、サブスクライブ、および構成するために TMA を使用できます。フィードは、指定された電子メール・アドレス宛に電子メールで、またはテキスト・ファイルとしても SFTP により、送信できます。

本オファリングは、「適格参加者」の課金単位に基づいてのみ適用されます。

1.2.3 IBM Trusteer Rapport Phishing Protection for Business および IBM Trusteer Rapport Phishing Protection for Retail

お客様 (および人数の制限なくお客様の有資格担当者) は、フィッシングが疑われるサイトまたは不正の可能性があるサイトへの「アカウント・ホルダー」のログイン資格情報の送信に関連するイベント・データ通知を受け取るために、TMA を使用することができます。正規のオンライン・アプリケーション (URL) に誤ってフィッシング・サイトのフラグが付けられることがあり、「クラウド・サービス」は正規サイトがフィッシング・サイトであると「アカウント・ホルダー」に警告する場合があります。このような場合、お客様は IBM にかかるエラーを通知し、IBM はかかるエラーを訂正する必要があります。これを、かかるエラーに対するお客様の唯一の救済策とします。

本「クラウド・サービス」は、「適格参加者」の課金単位、または「クライアント・デバイス」の課金単位に基づいて使用許諾されます。「法人向け」オファリングは、「適格参加者」10 人単位、または「クライアント・デバイス」10 個単位のパックで販売されています。「個人向け」オファリングは、「適格参加者」100 人単位、または「クライアント・デバイス」100 個単位のパックで販売されています。

本「クラウド・サービス」に対するプレミアム・サポートは、「適格参加者」の課金単位、または「クライアント・デバイス」の課金単位に基づいて取得することができます。「法人向け」オファリングは、「適格参加者」10 人単位、または「クライアント・デバイス」10 個単位のパックで販売されています。「個人向け」オファリングは、「適格参加者」100 人単位、または「クライアント・デバイス」100 個単位のパックで販売されています。

1.2.4 IBM Trusteer Rapport Mandatory Service for Business および IBM Trusteer Rapport Mandatory Service for Retail

お客様は、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「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) へアクセスする「適格参加者」への、「アカウント・ホルダーのクライアント・ソフトウェア」のダウンロードを義務付けるために、Trusteer Splash マーケティング・プラットフォームのインターフェースを使用することができます。

IBM Trusteer Rapport Premium Support for Business は、IBM Trusteer Rapport Mandatory Service for Business の前提条件です。

IBM Trusteer Rapport Premium Support for Retail は、IBM Trusteer Rapport Mandatory Service for Retail の前提条件です。

お客様は IBM Trusteer Rapport Mandatory Service の追加機能を導入することができますが、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「個人向けアプリケーション」または「法人向けアプリケーション」との併用のために、それが注文され、構成される場合に限ります。

本「クラウド・サービス」は、「適格参加者」の課金単位に基づいた権利を有します。「法人向け」オファリングは、10 単位のパックで販売されています。「個人向け」オファリングは、「適格参加者」100 人単位のパックで販売されています。

1.2.5 IBM Trusteer Rapport Additional Applications for Business および IBM Trusteer Rapport Additional Applications for Retail

IBM Trusteer Rapport II for Business について、1 つ目の「アプリケーション」以外の追加の「法人向けアプリケーション」に導入するには、IBM Trusteer Rapport Additional Applications for Business の「クラウド・サービス」の使用許諾が必要です。IBM Trusteer Rapport II for Retail について、1 つ目の「アプリケーション」以外の追加の「個人向けアプリケーション」に導入するには、IBM Trusteer Rapport Additional Applications for Retail の「クラウド・サービス」の使用許諾が必要です。

1.3 アクセラレーション・サービス

1.3.1 IBM Trusteer Rapport Large Redeployment および IBM Trusteer Rapport Small Redeployment

それぞれのオンライン・バンキング「アプリケーション」をサービスの期間中に再導入し、その結果として、IBM Trusteer Rapport II の導入に対する変更を必要とするお客様は、IBM Trusteer Rapport Redeployment の「クラウド・サービス」を購入する必要があります。

再導入は、お客様が「アプリケーション」のドメインまたはホスト URL を変更する、スプラッシュ構成に当該変更を適用する、または新しいオンライン・バンキング・プラットフォームへ移す場合に必要となります。

6 か月の再導入移行期間の間、お客様には、すでに申し込み済みの「アプリケーション」で実行する追加の「アプリケーション」について 1 対 1 で使用する権利があります。

IBM Trusteer Rapport Large Redeployment は 20,000 を超えるユーザーを持つ環境に適用され、IBM Trusteer Rapport Small Redeployment は 20,000 以下のユーザーを持つ環境に適用されます。

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 5.2 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。

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

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。

プレミアム・サポート

プレミアム・サポートのサブスクリプションは、本「クラウド・サービス」に対して追加料金で利用することができ、以下が含まれます。

- すべての重要度に対して英語による 1 日 24 時間 週 7 日のサポート。
- お客様は、電話およびコールバック・リクエストで直接サポートに連絡することができます。
- お客様およびその「適格参加者」は、「SaaS サポート・ハンドブック」に詳述されているとおり、電子的手段でサポート・チケットを送信することができます。
- お客様は以下のカスタマー・サポート・ポータルにアクセスして、通知、文書、事案レポート、および FAQ を確認することができます。http://www.ibm.com/software/security/trusteer/support/

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。

- 「エンゲージメント」とは、「クラウド・サービス」に関するプロフェッショナル・サービスまたはトレーニング・サービスです。
- 「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。
- 「アプリケーション」は、「クラウド・サービス」により開発される、または「クラウド・サービス」へアクセスするために提供されるか、「クラウド・サービス」で使用される、固有の名前が付けられたソフトウェア・プログラムです。

4.2 リモート・サービス料金

リモート・サービスを使用したか否かにかかわらず、リモート・サービスは購入日から 90 日後に満了となります。

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 EULA およびデータ主体のデータ処理に関する基準

IBM Trusteer Rapport クラウド・サービス (「Pinpoint クラウド・サービス」に関連して実施される場合、Rapport Remediation または Rapport for Mitigation が含まれます。) の場合: 別途の合意がある場合を除き、およびお客様が独自に設定した処理の基準に従って、お客様は、「ソフトウェア使用許諾契約」(https://trusteer.secure.force.com/PKB/articles/en_US/FAQ/RAPPORT-DATA-PRIVACY-NOTICE-AND-END-USER-LICENSE-AGREEMENT-EULA に掲載) を IBM が提供することを許可します。

IBM Trusteer クラウド・サービスの場合、お客様は、「支援企業」のデータ処理者である IBM が、マルウェアおよびマルウェア作成物 (すなわち、悪意のある行為に関連するファイル、または「プログラム」の異常な誤動作に関連するファイル) の収集のために「プログラム」を使用することを許可します。IBM は、エンド・ユーザーの個人情報が含まれているファイルを対象として「プログラム」を使用しません。ただし、収集されたファイルには、当該エンド・ユーザーの許可なくマルウェアによって取得された個人情報が含まれることがあります。IBM は、(1) 当該分析に関連しないファイルを直ちに削除し、かつ (2) 分析の期間 (いかなる場合も 3 か月以内) のみ関連するファイルを保持します。

5.2 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。

5.3 アカウント・ホルダーのデータ

明確にするために付言すると、特定の「アカウント・ホルダー」の「アカウント・ホルダー・クライアント・ソフトウェア」に関連する IBM のお客様 (かかる IBM のお客様を以下「関連顧客」といいます。) が複数あり、かつ異なる地域のデータセンターを通じてかかる「関連顧客」に IBM が本「サービス記述書」に基づくサービスを提供する場合、当該「アカウント・ホルダー」のデータは第 5.2 項に記載された各データセンターに関連するすべてのロケーションで処理することができます。

5.4 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。

5.5 イネーブリング・ソフトウェア

「クラウド・サービス」には以下の「イネーブリング・ソフトウェア」が含まれます。

- IBM Rapport Agents

5.6 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となる記録、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。

5.7 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、「クラウド・サービス」を改善する目的で「クラウド・サービス」の一部として、「コンテンツ」、および「コンテンツ」に由来するその他の情報 (「洞察」を除きます。) を使用します。IBM は、脅威の検知および保護の目的で「コンテンツ」に組み込まれた脅威 ID およびその他のセキュリティー情報も共有できます。