IBM Trusteer Fraud Protection

本「サービス記述書」は IBM がお客様に提供する「クラウド・サービス」について規定するものです。お客様とは、契約を結ぶ当事者、その許可ユーザーおよび「クラウド・サービス」の受領者を意味します。適用される「見積書」および「証書 (PoE)」は、別途「取引文書」として提供されます。

1. クラウド・サービス

以下の「クラウド・サービス」は、本「サービス記述書」の対象です。

Rapport クラウド・サービス:

- IBM Trusteer Rapport for Business
- IBM Trusteer Rapport for Business Premium Support
- IBM Trusteer Rapport for Retail
- 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 クラウド・サービス:

- IBM Trusteer Pinpoint Malware Detection for Business Standard Edition
- IBM Trusteer Pinpoint Malware Detection for Business Standard Edition Premium Support
- IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition
- IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition Premium Support
- IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition
- IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition Premium Support
- IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition
- IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition Premium Support
- IBM Trusteer Pinpoint Criminal Detection for Business
- IBM Trusteer Pinpoint Criminal Detection for Business Premium Support
- IBM Trusteer Pinpoint Criminal Detection for Retail
- IBM Trusteer Pinpoint Criminal Detection for Retail Premium Support
- IBM Trusteer Pinpoint Carbon Copy for Business

- IBM Trusteer Pinpoint Carbon Copy for Business Premium Support
- IBM Trusteer Pinpoint Carbon Copy for Retail
- IBM Trusteer Pinpoint Carbon Copy for Retail Premium Support
- IBM Trusteer Rapport Remediation for Retail
- IBM Trusteer Rapport Remediation for Retail Premium Support
- IBM Trusteer Pinpoint Criminal Detection II for Business
- IBM Trusteer Pinpoint Criminal Detection II for Retail
- IBM Trusteer Pinpoint Malware Detection II for Business Standard Edition
- IBM Trusteer Pinpoint Malware Detection II for Retail Standard Edition
- IBM Trusteer Pinpoint Malware Detection II for Business Advanced Edition
- IBM Trusteer Pinpoint Malware Detection II for Retail Advanced Edition
- IBM Trusteer Rapport Remediation for Business
- IBM Trusteer Rapport Remediation for Business Premium Support
- IBM Trusteer Pinpoint Criminal Detection Additional Applications for Retail
- IBM Trusteer Pinpoint Criminal Detection Additional Applications 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 Criminal Detection Redeployment
- 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 Pinpoint Detect Standard for Retail
- IBM Trusteer Pinpoint Detect Premium for Retail
- 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 with access management integration for Retail
- IBM Trusteer Pinpoint Detect Standard with access management integration for Business
- IBM Trusteer Pinpoint Detect Premium with access management integration for Retail
- IBM Trusteer Pinpoint Detect Premium with access management integration for Business
- IBM Trusteer Pinpoint Detect Standard Redeployment
- IBM Trusteer Pinpoint Detect Premium Redeployment
- IBM Trusteer Pinpoint Detect Standard For Retail Premium Support
- IBM Trusteer Pinpoint Detect Standard For Business Premium Support

Mobile クラウド・サービス:

- IBM Trusteer Mobile SDK for Business
- IBM Trusteer Mobile SDK for Retail
- IBM Trusteer Mobile Browser for Business
- IBM Trusteer Mobile Browser for Business Premium Support

- IBM Trusteer Mobile Browser for Retail
- IBM Trusteer Mobile Browser for Retail Premium Support

1.1 法人向けおよび個人向けのクラウド・サービス

IBM Trusteer Cloud Services は、特定タイプの「アプリケーション」との併用について使用許諾されています。「アプリケーション」は、「個人向け」または「法人向け」のどちらかのタイプと定義されます。「個人向けアプリケーション」および「法人向けアプリケーション」に対して、別々のオファリングが利用可能です。

a. 「個人向けアプリケーション」は、消費者にサービスを提供することを目的に設計されたオンライン・バンキング・アプリケーション、モバイル・アプリケーション、または e-コマース・アプリケーションと定義されます。お客様のポリシーによっては、特定の中小規模ビジネス向けのアプリケーションを、個人向けとして分類できる場合があります。

b. 「法人向けアプリケーション」は、法人、組織、もしくは同等の団体にサービスを提供することを目的に設計されたオンライン・バンキング・アプリケーション、モバイル・アプリケーション、もしくは e-コマース・アプリケーション、または「個人向け」に分類されないアプリケーションと定義されます。

1.1.1 法人向けのクラウド・サービス

- IBM Trusteer Rapport for Business
- IBM Trusteer Rapport II for Business
- IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition
- IBM Trusteer Pinpoint Malware Detection for Business Standard Edition
- IBM Trusteer Pinpoint Criminal Detection for Business
- IBM Trusteer Pinpoint Criminal Detection for Business Mobile
- IBM Trusteer Mobile SDK for Business
- IBM Trusteer Mobile Browser for Business
- IBM Trusteer Pinpoint Detect Standard for Business
- IBM Trusteer Pinpoint Detect Premium for Business
- IBM Trusteer Pinpoint Detect Standard with access management integration for Business
- IBM Trusteer Pinpoint Detect Premium with access management integration for Business

1.1.2 個人向けのクラウド・サービス

- IBM Trusteer Rapport for Retail
- IBM Trusteer Rapport II for Retail
- IBM Trusteer Pinpoint Criminal Detection for Retail
- IBM Trusteer Pinpoint Criminal Detection II for Retail
- IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition
- IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition
- IBM Trusteer Pinpoint Detect Standard for Retail
- IBM Trusteer Pinpoint Detect Premium for Retail
- IBM Trusteer Pinpoint Detect Standard with access management integration for Retail
- IBM Trusteer Pinpoint Detect Premium with access management integration for Retail
- IBM Trusteer Mobile SDK for Retail
- IBM Trusteer Mobile Browser for Retail

「法人向け」および「個人向け」の「クラウド・サービス」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 Mobile SDK の「クラウド・サービス」は除きます。

1.1.3 IBM Trusteer Rapport の追加の「クラウド・サービス」

a. IBM Trusteer Rapport 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 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 for Business または IBM Trusteer Rapport 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。

1.1.4 IBM Trusteer Pinpoint Malware Detection および IBM Trusteer Pinpoint Malware Detection の追加のクラウド・サービス

a. IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition もしくは IBM Trusteer Pinpoint Malware Detection for Business Standard Edition または IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business もしくは IBM Trusteer Pinpoint Malware Detection Standard Edition 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 Pinpoint Carbon Copy for Business
   - IBM Trusteer Rapport Remediation for Business
   - IBM Trusteer Pinpoint Malware Detection Additional Applications for Business

b. IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition もしくは IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition または IBM Trusteer Pinpoint Malware Detection II for Business Advanced Edition もしくは IBM Trusteer Pinpoint Malware Detection II for Business Standard Edition に対して利用可能な追加の「クラウド・サービス」
   - IBM Trusteer Pinpoint Carbon Copy for Retail
   - IBM Trusteer Rapport Remediation for Retail
   - IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail

本文書に記載される特定のオファリングについて、プレミアム・サポートが利用可能です。IBM Trusteer Pinpoint Malware Detection for Business もしくは IBM Trusteer Pinpoint Malware Detection for Retail または IBM Trusteer Pinpoint Malware Detection II for Business もしくは IBM Trusteer Pinpoint Malware Detection II for Retail のサブスクリプションは、本項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。

1.1.5 IBM Trusteer Pinpoint Criminal Detection および IBM Trusteer Pinpoint Criminal Detection II の追加のクラウド・サービス

a. IBM Trusteer Pinpoint Criminal Detection for Business または IBM Trusteer Pinpoint Criminal Detection II の追加の「クラウド・サービス」
   - IBM Trusteer Pinpoint Criminal Detection Additional Applications for Business

b. IBM Trusteer Pinpoint Criminal Detection for Retail および IBM Trusteer Pinpoint Criminal Detection II for Retail の追加の「クラウド・サービス」
   - IBM Trusteer Pinpoint Criminal Detection Additional Applications for Retail

本文書に記載される特定のオファリングについて、プレミアム・サポートが利用可能です。

IBM Trusteer Pinpoint Criminal Detection for Business もしくは IBM Trusteer Pinpoint Criminal Detection for Retail または IBM Trusteer Pinpoint Criminal Detection II for Business もしくは IBM Trusteer Pinpoint Criminal Detection II for Retail のサブスクリプションは、本項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。

1.1.6 IBM Trusteer Pinpoint Detect Standard および IBM Trusteer Pinpoint Detect Premium ならびに IBM Security Pinpoint Detect Standard with access management integration および IBM Security Detect Premium with access management integration の追加のクラウド・サービス

a. IBM Trusteer Detect Standard for Business および IBM Trusteer Pinpoint Detect Premium for Business ならびに IBM Security Pinpoint Detect Standard with access management integration for Business および IBM Security Detect Premium with access management integration for Business の追加の「クラウド・サービス」
   - IBM Trusteer Pinpoint Detect Standard Additional Applications for Business
   - IBM Trusteer Pinpoint Detect Premium Additional Applications for Business

b. IBM Trusteer Detect Standard for Retail および IBM Trusteer Pinpoint Detect Premium for Retail ならびに IBM Security Pinpoint Detect Standard with access management integration for Retail および IBM Security Detect Premium with access management integration for Retail の追加の「クラウド・サービス」
   - IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail
   - IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail

IBM Trusteer Detect Standard もしくは IBM Trusteer Pinpoint Detect Premium または IBM Security Pinpoint Detect Standard with access management integration もしくは IBM Security Detect Premium with access management integration のサブスクリプションは、本項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。

1.1.7 その他の追加のクラウド・サービス

上記の基本サブスクリプションの追加の「クラウド・サービス」サブスクリプションのうち、本書に記載されていないものは、現在利用可能であるか開発中であるかにかかわらず、更新とはみなされず、別途、許可を受ける必要があります。

1.2 定義

「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 (「EULA」) 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、もしくは IBM Trusteer Mobile Browser 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上で行うインストールのための「クラウド・サービス」の一部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。

「Trusteer Splash」とは、利用可能な Splash テンプレートに基づいてお客様に提供されるスプラッシュをいいます。

「ランディング・ページ」とは、IBM がホストするページのうち、お客様のスプラッシュおよびダウンロード可能な「アカウント・ホルダーのクライアント・ソフトウェア」と共にお客様に提供されるものをいいます。

2. IBM Trusteer Rapport のクラウド・サービス

2.1 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、「対象参加者」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、「対象参加者」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、「対象参加者」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お客様の有資格担当者) 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) ソフトウェア使用許諾契約 (以下「EULA」といいます。) に基づいてお客様の「対象参加者」に無償で使用許諾されており、「対象参加者」のデスクトップやデバイス (PC または MAC) にダウンロードできるようになっている、Trusteer Rapport ソフトウェア・スイートとも呼ばれるクライアント・イネーブリング・ソフトウェア (以下「アカウント・ホルダーのクライアント・ソフトウェア」といいます。) 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。

b. Web スクリプト

「クラウド・サービス」にアクセスするため、またはそれを使用するための、Web サイト上でのアクセス用。

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「対象参加者」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「対象参加者」が特定され、当該「対象参加者」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 と関連して用いるために、および、Trusteer Splash での利用ならびに「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 IBM Trusteer Web サイト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だけに、自社の商標、ロゴ、またはアイコンを提供することに同意することができます。お客様から提供された商標、ロゴ、またはアイコンの使用は、広告および商標の使用に関する IBM の合理的なポリシーに従うものとします。

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。「対象参加者」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。

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

「Trusteer Rapport II」の「クラウド・サービス」は、複数の「アプリケーション」の保護に関連する料金の標準化を支援する IBM Trusteer Rapport の新規体系であり、「アプリケーション」を追加する際に 1 回限りの料金に取って代わります。

「Trusteer Rapport II」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」は、「対象参加者」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、「対象参加者」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、「対象参加者」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お客様の有資格担当者) 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) ソフトウェア使用許諾契約 (以下「EULA」といいます。) に基づいてお客様の「対象参加者」に無償で使用許諾されており、「対象参加者」のデスクトップやデバイス (PC または MAC) にダウンロードできるようになっている、Trusteer Rapport ソフトウェア・スイートとも呼ばれるクライアント・イネーブリング・ソフトウェア (以下「アカウント・ホルダーのクライアント・ソフトウェア」といいます。) 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。

b. Web スクリプト

   「クラウド・サービス」にアクセスするため、またはそれを使用するための、Web サイト上でのアクセス用。

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「対象参加者」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「対象参加者」が特定され、当該「対象参加者」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 と関連して用いるために、および、Trusteer Splash での利用ならびに「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 IBM Trusteer Web サイト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だけに、自社の商標、ロゴ、またはアイコンを提供することに同意することができます。お客様から提供された商標、ロゴ、またはアイコンの使用は、広告および商標の使用に関する IBM の合理的なポリシーに従うものとします。

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。「対象参加者」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。

Trusteer Rapport II for Business および Trusteer Rapport II for Retail にはそれぞれ 1 つの「アプリケーション」の保護が含まれます。追加的な「アプリケーション」のそれぞれについては、お客様は、IBM Trusteer Rapport Additional Application の使用許諾を取得する必要があります。

2.3 IBM Trusteer Rapport for Business および IBM Trusteer Rapport for Retail ならびに IBM Trusteer Rapport II for Business および IBM Trusteer Rapport II for Retail に関するオプションの追加のクラウド・サービス

IBM Trusteer Rapport の「クラウド・サービス」または IBM Trusteer Rapport II の「クラウド・サービス」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「対象参加者」(「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。

2.3.1 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。

2.3.2 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。

2.3.3 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「対象参加者」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 Security Rapport Mandatory Service for Business の前提条件です。

IBM Trusteer Rapport Premium Support for Retail は、IBM Security 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。

2.3.4 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 または 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。

2.3.5 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、最初の「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、最初の「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。

3. IBM Trusteer Pinpoint のクラウド・サービス

IBM Trusteer Pinpoint はクラウド・ベース・サービスで、別の保護層を提供できるように設計されており、マルウェア攻撃、フィッシング攻撃、およびアカウント乗っ取り攻撃を検出して抑制することを目的としています。Trusteer Pinpoint は、お客様が申し込んでいる「クラウド・サービス」の範囲および不正防止プロセスの対象である、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) に統合することができます。

本「クラウド・サービス」には以下が含まれます。

a. TMA

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) Pinpoint オファリング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、および構成することができます。

b. Web スクリプトおよび API

「クラウド・サービス」にアクセスするため、またはそれを使用するための、Web サイト上での導入用。

3.1 IBM Trusteer Pinpoint Malware Detection および IBM Trusteer Pinpoint Criminal Detection

IBM Trusteer Pinpoint Malware Detection の「クラウド・サービス」もしくは IBM Trusteer Pinpoint Malware Detection II の「クラウド・サービス」においてマルウェアが検出された場合、または IBM Trusteer Pinpoint Criminal Detection の「クラウド・サービス」もしくは IBM Trusteer Pinpoint Criminal Detection II の「クラウド・サービス」においてアカウント乗っ取りが検出された場合、お客様は「Pinpoint ベスト・プラクティス・ガイド」に従う必要があります。IBM Trusteer Pinpoint Malware Detection の「クラウド・サービス」、IBM Trusteer Pinpoint Malware Detection II の「クラウド・サービス」、IBM Trusteer Pinpoint Criminal Detection の「クラウド・サービス」、IBM Trusteer Pinpoint Criminal Detection II の「クラウド・サービス」については、マルウェア検出またはアカウント乗っ取り検出の直後に、第三者がお客様のアクションを IBM Trusteer Pinpoint クラウド・サービスに結び付けてしまうような影響を「対象参加者」の経験に及ぼすような形で使用しないでください (例: マルウェア検出またはアカウント乗っ取り検出の直後の通知、メッセージ、デバイスのブロック、「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アクセスのブロック)。

3.2 IBM Trusteer Pinpoint Criminal Detection for Business および IBM Trusteer Pinpoint Criminal Detection for Retail

デバイス ID、フィッシング検出、およびマルウェアによる資格情報の窃取検出を用いることで、「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」に接続しているブラウザーのアカウント乗っ取りが疑われる活動のクライアントレス検出を行います。IBM Trusteer Pinpoint Criminal Detection の「クラウド・サービス」は、別の保護層を提供します。また、アカウント乗っ取りの試みを検出して、「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」に (ネイティブ・ブラウザーまたはお客様のモバイル・アプリケーションを介して) アクセスするブラウザーまたはモバイル・デバイスのリスク評価スコアをお客様に直接提供することを目的としています。

a. 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「対象参加者」との間のオンライン対話の結果として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。または、お客様はバックエンド API 提供モードにより、イベント・データを受け取ることができます。

3.3 IBM Trusteer Pinpoint Criminal Detection II for Business および IBM Trusteer Pinpoint Criminal Detection II for Retail

IBM Security Pinpoint Criminal Detection II は、複数の「アプリケーション」の保護に関連する料金の標準化を支援する IBM Trusteer Pinpoint Criminal Detection の新規体系であり、「アプリケーション」を追加する際に 1 回限りの料金に取って代わります。

デバイス ID、フィッシング検出、およびマルウェアによる資格情報の窃取検出を用いることで、「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」に接続しているブラウザーのアカウント乗っ取りが疑われる活動のクライアントレス検出を行います。IBM Trusteer Pinpoint Criminal Detection II の「クラウド・サービス」は、別の保護層を提供します。また、アカウント乗っ取りの試みを検出して、「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」に (ネイティブ・ブラウザーまたはお客様のモバイル・アプリケーションを介して) アクセスするブラウザーまたはモバイル・デバイスのリスク評価スコアをお客様に直接提供することを目的としています。

a. 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「対象参加者」との間のオンライン対話の結果として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。または、お客様はバックエンド API 提供モードにより、イベント・データを受け取ることができます。

本「クラウド・サービス」には 1 つの「アプリケーション」の保護が含まれます。追加的な「アプリケーション」のそれぞれについては、お客様は、IBM Trusteer Pinpoint Criminal Detection Additional Applications の使用許諾を取得する必要があります。

3.4 IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition および IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition および IBM Trusteer Pinpoint Malware Detection for Business Standard Edition および IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition

「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」に接続するブラウザーの、金融関連の MITB (マン・イン・ザ・ブラウザー) マルウェア感染のクライアントレス検出。IBM Trusteer Pinpoint Malware Detection の「クラウド・サービス」は、別の保護層を提供します。また、金融関連の MITB マルウェアの存在について、お客様に評価および警告を提供することにより、組織・団体がマルウェアのリスクに基づいて不正防止プロセスに重点的に取り組めるようにすることを目的としています。

a. 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」と「対象参加者」との間のオンライン対話の結果として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。

b. Advanced Edition

Advanced Edition for Business および Advanced Edition for Retail (またはそのいずれか) は、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) の構成およびフローに合わせて調整、カスタマイズされた、検出および保護の追加の層を提供します。また、お客様を標的とした特別な脅威の状況に合わせてカスタマイズすることができます。これは、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) のさまざまな領域に組み込むことができます。

Advanced Edition は、少なくとも「個人向け対象参加者」100,000 人または「法人向け対象参加者」10,000 人を最低数量として、お客様に提供されます。つまり、Advanced Edition for Retail の場合は、「対象参加者」100 人単位のパックが 1,000 パック、Advanced Edition for Business の場合は、「対象参加者」10 人単位のパックが 1,000 パックに相当します。

c. Standard Edition

Standard Edition for Business または Standard Edition for Retail は、本書に記載のとおり、本「クラウド・サービス」のコア機能を提供する、迅速な導入が可能なソリューションです。

3.5 IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business および IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail ならびに IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business および IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail

IBM Security Pinpoint Malware Detection II は、複数の「アプリケーション」の保護に関連する料金の標準化を支援する IBM Trusteer Pinpoint Malware Detection の新規体系であり、「アプリケーション」を追加する際に 1 回限りの料金に取って代わります。

「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」に接続するブラウザーの、金融関連の MITB (マン・イン・ザ・ブラウザー) マルウェア感染のクライアントレス検出。IBM Trusteer Pinpoint Malware Detection の「クラウド・サービス」は、別の保護層を提供します。また、金融関連の MITB マルウェアの存在について、お客様に評価および警告を提供することにより、組織・団体がマルウェアのリスクに基づいて不正防止プロセスに重点的に取り組めるようにすることを目的としています。

a. 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」と「対象参加者」との間のオンライン対話の結果として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。

b. Advanced Edition

Advanced Edition for Business および Advanced Edition for Retail (またはそのいずれか) は、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) の構成およびフローに合わせて調整、カスタマイズされた、検出および保護の追加の層を提供します。また、お客様を標的とした特別な脅威の状況に合わせてカスタマイズすることができます。これは、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) のさまざまな領域に組み込むことができます。

Advanced Edition は、少なくとも「個人向け対象参加者」100,000 人または「法人向け対象参加者」10,000 人を最低数量として、お客様に提供されます。つまり、Advanced Edition for Retail の場合は、「対象参加者」100 人単位のパックが 1,000 パック、Advanced Edition for Business の場合は、「対象参加者」10 人単位のパックが 1,000 パックに相当します。

c. Standard Edition

Standard Edition for Business または Standard Edition for Retail は、本書に記載のとおり、本「クラウド・サービス」のコア機能を提供する、迅速な導入が可能なソリューションです。

本「クラウド・サービス」には 1 つの「アプリケーション」の保護が含まれます。追加的な「アプリケーション」のそれぞれについては、お客様は、IBM Trusteer Pinpoint Malware Detection Additional Applications の使用許諾を取得しなければなりません。

3.6 Cloud Trusteer Pinpoint Malware Detection for Business Advanced Edition および IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition ならびに IBM Trusteer Pinpoint Malware Detection for Business Standard Edition および IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition ならびに IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail および IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business ならびに IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail および IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business の任意の追加のクラウド・サービス

- IBM Trusteer Rapport Remediation for Retail の「クラウド・サービス」については、IBM Trusteer Pinpoint Malware Detection Standard Edition for Retail、IBM Trusteer Pinpoint Malware Detection Advanced Edition for Retail、IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail、IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail のいずれかを前提条件とします。
- IBM Trusteer Rapport Remediation for Business の「クラウド・サービス」については、IBM Trusteer Pinpoint Malware Detection Standard Edition for Business、IBM Trusteer Pinpoint Malware Detection Advanced Edition for Business、IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business、IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business のいずれかを前提条件とします。
- IBM Trusteer Pinpoint Carbon for Retail については、IBM Trusteer Pinpoint Malware Detection Standard Edition for Retail、IBM Trusteer Pinpoint Malware Detection Advanced Edition for Retail、IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail、IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail のいずれかを前提条件とします。
- IBM Trusteer Pinpoint Carbon Copy for Business については、IBM Trusteer Pinpoint Malware Detection Standard Edition for Business、IBM Trusteer Pinpoint Malware Detection Advanced Edition for Business、IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business、IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business のいずれかを前提条件とします。

3.6.1 IBM Trusteer Pinpoint Carbon Copy for Business および IBM Trusteer Pinpoint Carbon Copy for Retail

IBM Trusteer Pinpoint Carbon Copy オファリングは、別の保護層および監視サービスを提供できるように設計されています。この監視サービスは、お客様が申し込んでいる「クラウド・サービス」オファリング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」に対して行われたフィッシング攻撃によって「対象参加者」の資格情報が漏えいしたことを特定するのに役立ちます。

3.6.2 IBM Trusteer Rapport Remediation for Retail および IBM Trusteer Rapport Remediation for Business

IBM Trusteer Rapport Remediation for Retail および IBM Trusteer Rapport Remediation for Business は、IBM Trusteer Pinpoint Malware Detection のイベント・データによって MITB マルウェアが 検出された場合に、限定的にお客様の「アプリケーション」にアクセスするお客様の「対象参加者」が所有する感染したデバイス (PC または MAC) を対象に MITB (マン・イン・ザ・ブラウザー) マルウェア感染を調査、処置、ブロック、および駆除することを目的としています。お客様は、お客様の「アプリケーション」上で実際に稼働している IBM Trusteer Pinpoint Malware Detection または IBM Trusteer Pinpoint Malware Detection II に対して有効なサブスクリプションを有している必要があります。お客様は、お客様の「アプリケーション」にアクセスする「対象参加者」に関連してのみ、かつ特定の感染したデバイス (PC または MAC) を限定的に調査、処置するためのツールとしてのみ、本「クラウド・サービス」オファリングを利用することができます。IBM Trusteer Rapport Remediation は、かかる感染した「対象参加者」のデバイス (PC または MAC) 上で実際に稼働する必要があり、かつかかる感染した「対象参加者」が EULA を受諾し、お客様の「アプリケーション」で少なくとも 1 回は認証を受けていなければなりません。また、お客様の設定には、ユーザー ID の収集が含まれている必要があります。明確にするために記すと、本「クラウド・サービス」オファリングには、Trusteer Splash の使用権およびお客様の一般的な「対象参加者」全般に対してその他の方法で「アカウント・ホルダーのクライアント・ソフトウェア」利用を促す権利 (またはそのいずれか) は含まれていません。

3.6.3 IBM Trusteer Pinpoint Malware Detection 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 Pinpoint Malware Detection および IBM Trusteer Pinpoint Malware Detection II またはそのいずれかの導入に対する変更を必要とするお客様は、IBM Trusteer Pinpoint Malware Detection Redeployment 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、オンライン「アプリケーション」を新規テクノロジーに変換する、新しいオンライン・バンキング・プラットフォームへ移す、または既存の「アプリケーション」に新規ログイン・フローを追加する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。

3.6.4 IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail および IBM Trusteer Pinpoint Malware Detection Additional Applications for Business

IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business または IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business について、最初の「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 Pinpoint Malware Detection Additional Applications for Business の使用許諾が必要です。IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail または IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail について、最初の「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 Pinpoint Malware Detection Additional Applications for Retail の使用許諾が必要です。

3.7 IBM Trusteer Pinpoint Criminal Detection for Business および IBM Trusteer Pinpoint Criminal Detection for Retail ならびに IBM Trusteer Pinpoint Criminal Detection II for Business および IBM Trusteer Pinpoint Criminal Detection II for Retail のオプションの追加のクラウド・サービス

3.7.1 IBM Trusteer Pinpoint Criminal Detection 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 Pinpoint Criminal Detection の「クラウド・サービス」の導入に対する変更を必要とするお客様は、IBM Trusteer Pinpoint Criminal Detection Redeployment 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、オンライン「アプリケーション」を新規テクノロジーに変換する、新しいオンライン・バンキング・プラットフォームへ移す、または既存の「アプリケーション」に新規ログイン・フローを追加する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。

3.7.2 IBM Trusteer Pinpoint Criminal Detection Additional Applications for Business および IBM Trusteer Pinpoint Criminal Detection Additional Applications for Retail

IBM Trusteer Pinpoint Criminal Detection II for Business について、最初の「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 Pinpoint Criminal Detection Additional Applications for Business の使用許諾が必要です。IBM Trusteer Pinpoint Criminal Detection II for Retail について、最初の「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 Pinpoint Criminal Detection Additional Applications for Retail の使用許諾が必要です。

4. IBM Trusteer Fraud Protection Suite

IBM Trusteer Fraud Protection Suite (以下「スイート」といいます。) は、不正からの保護層を提供するように設計されたクラウド・ベースの一連のサービスをいい、追加的な IBM 製品と統合して、ライフサイクル管理ソリューションを提供することができます。 「スイート」には、以下のクラウド・ベース・サービスが含まれます。

- マルウェア攻撃、フィッシング攻撃、およびアカウント乗っ取り攻撃を検出して抑制することを目的とした IBM Trusteer Pinpoint Detect。Trusteer Pinpoint Detect は、お客様が申し込んでいる「クラウド・サービス」の範囲および不正防止プロセスの対象である、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) に統合することができます。
- 感染したエンドポイントの処置および保護を目的とした IBM Trusteer Rapport for Mitigation

「クラウド・サービス」には以下が含まれます。

a. TMA

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) イベント・データ報告およびリスク評価を受け取ること、(ii) セキュリティー・ポリシーや、イベント・データの報告に関連するポリシーの表示・構成・設定を行うことができます。

b. 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「対象参加者」との間のオンライン対話の結果として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。または、お客様はバックエンド API 提供モードにより、イベント・データを受け取ることができます。

c. Web スクリプトおよび API

「クラウド・サービス」にアクセスするため、またはそれを使用するための、Web サイト上での導入用。

Pinpoint ベスト・プラクティス

マルウェア検出またはアカウント乗っ取り検出の場合、お客様は、「Pinpoint ベスト・プラクティス・ガイド」に従う必要があります。IBM Trusteer Pinpoint Detect の「クラウド・サービス」については、マルウェア検出またはアカウント乗っ取り検出の直後に、第三者がお客様のアクションを IBM Trusteer Pinpoint Detect オファリングに結び付けてしまうような影響を「対象参加者」の経験に及ぼすような形で使用しないでください (例: マルウェア検出またはアカウント乗っ取り検出の直後の通知、メッセージ、デバイスのブロック、「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アクセスのブロック)。

4.1 IBM Trusteer Pinpoint Detect Standard for Business および IBM Trusteer Pinpoint Detect Standard for Retail

この「クラウド・サービス」は、IBM Trusteer Pinpoint Criminal Detection と IBM Trusteer Pinpoint Malware Detection の両「クラウド・サービス」を組み合わせて、単一の一元化されたソリューションとして提供します。

このソリューションは、デバイス ID、フィッシング検出、およびマルウェアによる資格情報の窃取検出を用いることで、「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」に接続しているブラウザーに対するマルウェアまたはアカウント乗っ取りが疑われる活動のクライアントレス検出を容易にします。IBM Trusteer Pinpoint オファリングは、別の保護層を提供します。また、アカウント乗っ取りの試みを検出して、「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」に (ネイティブ・ブラウザーまたはお客様のモバイル・アプリケーションを介して) アクセスするブラウザーまたはモバイル・デバイスのリスク評価スコアをお客様に直接提供することを目的としています。

この「クラウド・サービス」には、標準サポート (下記のテクニカル・サポート項に規定) が含まれています。プレミアム・サポートについては、お客様は Detect Premium を購入する必要があります。

本「クラウド・サービス」には 1 つの「アプリケーション」の保護が含まれます。追加的な「アプリケーション」のそれぞれについては、お客様は、IBM Trusteer Pinpoint Detect Standard Additional Applications の使用許諾を取得する必要があります。

4.2 IBM Trusteer Pinpoint Detect Premium for Business および IBM Trusteer Pinpoint Detect Premium for Retail

本「クラウド・サービス」は、IBM Trusteer Pinpoint Criminal Detection と IBM Trusteer Pinpoint Malware Detection を組み合わせて、単一の容易に統合できる一元化されたソリューションとし、拡張された機能およびサービス (拡張された導入およびセットアップ・サービス、カスタマイズされたセキュリティー・ポリシー、調査サービスなど) と共に提供します。

本「クラウド・サービス」には 1 つの「アプリケーション」の保護が含まれます。追加的な「アプリケーション」のそれぞれについては、お客様は、IBM Trusteer Pinpoint Detect Premium Additional Applications の使用許諾を取得する必要があります。

この「クラウド・サービス」にはプレミアム・サポートが含まれています。

4.3 IBM Trusteer Pinpoint Detect Standard with access management integration for Business および IBM Trusteer Pinpoint Detect Standard with access management integration for Retail

IBM Trusteer Pinpoint Detect Standard with access management integration の「クラウド・サービス」には、上記の第 4.1 項に詳述されている IBM Security Pinpoint Detect Standard の機能が含まれます。

IBM Trusteer Pinpoint Detect Standard with access management integration は、IBM Security Access Management (以下「ISAM」といいます。) などのアクセス管理システムと共に購入された場合に使用されます。ISAM と共に購入された場合、両オファリングは有効化されなければなりません。このオファリングにはアクセス管理システムとの統合オプションが含まれています。アクセス管理システム用の使用許諾は含まれていません。

本オファリングには 1 つの「アプリケーション」の保護が含まれます。追加的な「アプリケーション」のそれぞれについては、お客様は、IBM Trusteer Pinpoint Detect Standard Additional Applications の使用許諾を取得する必要があります。

本「クラウド・サービス」には、標準サポート (テクニカル・サポート項に規定) が含まれています。
IBM Trusteer Pinpoint Detect Premium with access management integration for Business および IBM Trusteer Pinpoint Detect Premium with access management integration for Retail

IBM Trusteer Pinpoint Detect Premium with access management integration の「クラウド・サービス」には、上記の第 4.2 項に詳述されている IBM Security Pinpoint Detect Premium の機能、およびアクセス管理システムとの統合オプションが含まれます。

IBM Trusteer Pinpoint Detect Premium with access management integration は、IBM Security Access Management (以下「ISAM」といいます。) などのアクセス管理システムと共に購入された場合に使用されます。ISAM と共に購入された場合、両オファリングは有効化されなければなりません。本「クラウド・サービス」にはアクセス管理システムとの統合オプションが含まれています。アクセス管理システム用の使用許諾は含まれていません。

本「クラウド・サービス」には 1 つの「アプリケーション」の保護が含まれます。追加的な「アプリケーション」のそれぞれについては、お客様は、IBM Trusteer Pinpoint Detect Premium Additional Applications の使用許諾を取得する必要があります。

本オファリングにはプレミアム・サポートが含まれています。

4.4 IBM Trusteer Pinpoint Detect Standard および IBM Trusteer Pinpoint Detect Premium のオプション・サービス

本項に含まれた「クラウド・サービス」については、IBM Trusteer Pinpoint Detect Premium for Retail または IBM Trusteer Pinpoint Detect Standard for Retail に対する使用許諾が前提条件となります。

4.5 IBM Trusteer Rapport for Mitigation for Retail および IBM Trusteer Rapport for Mitigation for Business

IBM Trusteer Rapport for Mitigation は、IBM Trusteer Pinpoint Detect Premium または IBM Trusteer Pinpoint Detect Standard のイベント・データによってマルウェア感染が検出された場合に、限定的にお客様の「個人向けアプリケーション」にアクセスするお客様の「対象参加者」が所有する感染したデバイス (PC または MAC) を対象にマルウェア感染を調査、処置、ブロック、および駆除することを目的としています。お客様は、お客様の「個人向けアプリケーション」上で実際に稼働している IBM Trusteer Pinpoint Detect Premium または IBM Trusteer Pinpoint Detect Standard に対して有効なサブスクリプションを有している必要があります。お客様は、お客様の「個人向けアプリケーション」にアクセスする「対象参加者」に関連してのみ、かつ特定の感染したデバイス (PC または MAC) を限定的に調査、処置するためのツールとしてのみ、本「クラウド・サービス」を利用することができます。IBM Trusteer Rapport for Mitigation for Retail は、かかる感染した「対象参加者」のデバイス (PC または MAC) 上で実際に稼働する必要があり、かつかかる感染した「対象参加者」が EULA を受諾し、お客様の「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なければなりません。また、お客様の設定には、ユーザー ID の収集が含まれている必要があります。明確にするために記すと、この「クラウド・サービス」には、Trusteer Splash の使用権およびお客様の一般的な「対象参加者」に対してその他の方法で「アカウント・ホルダーのクライアント・ソフトウェア」の利用を促す権利 (またはそのいずれか) は含まれていません。

4.5.1 IBM Trusteer Pinpoint Detect Standard Additional Applications for Business および IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail ならびに IBM Trusteer Pinpoint Detect Premium Additional Applications for Business および IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail

IBM Trusteer Pinpoint Standard for Business について、最初の「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 Pinpoint Detect Standard Additional Applications for Business の使用許諾が必要です。

IBM Trusteer Pinpoint Standard for Retail について、最初の「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 Pinpoint Detect Standard Additional Applications for Retail の使用許諾が必要です。

IBM Trusteer Pinpoint Premium for Business について、最初の「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 Pinpoint Detect Premium Additional Applications for Business の使用許諾が必要です。

IBM Trusteer Pinpoint Premium for Retail について、最初の「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 Pinpoint Detect Premium Additional Applications for Retail の使用許諾が必要です。

4.5.2 IBM Trusteer Pinpoint Detect Standard Redeployment および IBM Trusteer Pinpoint Detect Premium 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 Pinpoint Detect の導入に対する変更を必要とするお客様は、IBM Trusteer Pinpoint Detect Redeployment 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、オンライン「アプリケーション」を新規テクノロジーに変換する、新しいオンライン・バンキング・プラットフォームへ移す、または既存の「アプリケーション」に新規ログイン・フローを追加する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。

5. IBM Trusteer Mobile のクラウド・サービス

5.1 IBM Trusteer Mobile Browser for Business および IBM Trusteer Mobile Browser for Retail

IBM Trusteer Mobile Browser は、別の保護層を追加できるように設計されています。また、お客様が申し込んでいる「クラウド・サービス」の範囲、モバイル・デバイスのリスク評価、およびフィッシング保護の対象である、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」にアクセスする、「対象参加者」のモバイル・デバイスについて安全なオンライン・アクセスを提供することを目的としています。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。本「クラウド・サービス」の場合、モバイル・デバイスにはスマートフォンまたはタブレットが含まれ、ラップトップ PC および Mac は含まれません。

TMA により、お客様は、「対象参加者」が、(i)ソフトウェア使用許諾契約 (「EULA」) に基づいて一般に無償で使用許諾され、「対象参加者」のモバイル・デバイスにダウンロードできるようになっているアプリケーションである「アカウント・ホルダーのクライアント・ソフトウェア」をダウンロード済みで、(ii) EULA を受諾し、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」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、デバイスに関連するイベント・データ、分析、および統計情報を受け取ることができます。お客様は、Trusteer Splash 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。また、社内業務の実行に「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。

a. 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、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」とモバイル・デバイスとの間のオンライン対話の結果として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。

b. 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「対象参加者」が特定され、当該「対象参加者」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 (以下「Splash テンプレート」といいます。) 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 と関連して用いるために、および、Trusteer Splash での利用ならびに「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 IBM によりホストされるランディング・ページ上もしくは IBM Trusteer Web サイト上で表示するためだけに、自社の商標、ロゴ、またはアイコンを提供することに同意することができます。お客様から提供された商標、ロゴ、またはアイコンの使用は、広告および商標の使用に関する IBM の合理的なポリシーに従うものとします。

5.2 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、およびファーミング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、「対象参加者」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、「対象参加者」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。「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「対象参加者」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. 「対象参加者」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) 強制法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・オファリング」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 Trusteer Mobile SDK で提供されるモバイル・ツール (以下「モバイル・ツール」といいます。) を用いて作成されたサンプル・アプリケーションを Apple (iOS)、Google (Android)、およびその他のモバイル・オペレーティング・システム・プラットフォーム (以下、総称して「モバイル OS プラットフォーム」といいます。) の特定バージョンで適切に実行できるかどうかを判断するために確認を行っていますが、「モバイル OS プラットフォーム」は第三者によって提供されるものであり、IBM の管理下にないため、IBM への通知なく変更される場合があります。このため、これに反する条項にかかわらず、モバイル・ツールを使用して作成されるアプリケーションまたはその他の出力がモバイル OS プラットフォームまたはモバイル・デバイスで適切に実行もしくは相互運用されること、またはその互換性について IBM は保証するものではありません。

「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、サポートの義務を負わずに現状のままの状態で「ソース・コンポーネント」および「サンプル資料」を提供するものであり、権原の保証、第三者の権利の不侵害の保証、特許権の不侵害の保証、ならびに商品性および特定目的適合性に関する黙示の保証を含む (ただし、これらに限定されません。)、明示または黙示のいかなる保証もしません。「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。

お客様は、お客様による IBM Trusteer Mobile SDK の使用が本「サービス記述書」の条件に準拠していることについて監査可能な確認を実施するために十分な、正確な書面による記録、システム・ツールの出力、およびその他システム情報を作成し、保持し、IBM およびその監査人に提供することに同意するものとします。

6. プレミアム・サポート

お客様は、お客様が申し込んでいる関連プレミアム・サポート・オファリングの対象である「クラウド・サービス」に対してのみ、プレミアム・サポートを受ける権利を有します。

7. IBM Trusteer Fraud Protection の導入

お客様が申し込む「アプリケーション」のそれぞれについて、お客様の基本的なサブスクリプションには、IBM Trusteer クラウド上での必要なセットアップおよび初回の導入活動 (初回のワンタイム・スタートアップ、構成、「Splash テンプレート」、テスト、およびトレーニングなど) が含まれています。

導入作業には、お客様の「アプリケーション」やシステム上で必要とされる実装活動は含まれません。

各種「クラウド・サービス」の実装フェーズは、関連する導入ガイドに詳述された期限で実装できるように設計されています。

割り当てられた期限内にこうした実装フェーズを完了することは、お客様の管理職および要員の全面的な関与と参加に依存しています。お客様は、タイムリーに必要な情報を提供する必要があります。IBM のパフォーマンスは、お客様の時宜を得た情報および意思決定に基づくため、遅延は追加費用の発生、および、こうした実装サービスの完了の遅延、またはそのいずれかにつながる可能性があります。

お客様が申し込む「アプリケーション」のそれぞれについて、お客様の基本的なサブスクリプションには、IBM Trusteer クラウド上での必要なセットアップおよび初回の導入活動 (初回のワンタイム・スタートアップ、構成、「Splash テンプレート」、テスト、およびトレーニングなど) が含まれています。

お客様のサブスクリプションには、初回の導入で IBM の助言に従ってタグ付けされる、お客様のアプリケーション内のページに対するサポートおよびテストが含まれます。IBM は以下について責任を負いません。(i) 部分的な導入、(ii) お客様が、IBM の推奨事項に従った IBM クラウド・サービスの導入を選択しない場合、および (iii) お客様が、自ら単独で導入、セットアップ、およびテストを実行することを選択した場合。(IV) 一部の導入または保護がお客様が提供した不適切な情報の結果である場合。初回の導入以外の導入作業を含めて、追加のサービスは、追加料金にて、別途合意書に基づいた契約の対象となる場合があります。

8. データのプライバシーおよびセキュリティー

本「クラウド・サービス」は、IBM の「IBM SaaS」に関する「Data Security and Privacy Principles」(http://www.ibm.com/cloud/data-security で入手可能) および本セクションの追加条件に従うものとします。IBM の「Data Security and Privacy Principles」が変更される場合であっても、それにより「クラウド・サービス」のセキュリティーのレベルが低下することはありません。

保護対象のデータの処理およびデータの特性により提示されるリスクに対して技術的および組織上のセキュリティー対策が適切であると、お客様がデータ管理者として判断する場合には、本「クラウド・サービス」を使用して、個人データが含まれるコンテンツを処理することができます。お客様は、本「クラウド・サービス」ではセンシティブ個人データや追加の規制要件の対象となるデータを保護するためのフィーチャーが提供されないことを認識しています。

本「クラウド・サービス」は、IBM プライバシー・シールド認定に含まれ、お客様が「クラウド・サービス」を米国に在るデータセンターでホストすることを選択した場合に、IBM の「Privacy Shield Privacy Policy」(http://www.ibm.com/privacy/details/us/en/privacy_shield.html に掲載) が適用されます。

8.1 セキュリティー機能および責任

「クラウド・サービス」には、以下のセキュリティー機能が実装されています。

「クラウド・サービス」では、IBM ネットワークを伝送先および伝送元とするデータ伝送中に、ならびにエンドポイントからのデータ伝送を待機中に、コンテンツを暗号化します。

8.2 合法的使用および同意

合法的使用

本「クラウド・サービス」の利用は、あらゆる法律または規則に関係する場合があります。「クラウド・サービス」は、合法的目的かつ合法的方法による場合にのみ利用可能です。お客様は、適用される法律、規則、および方針に従って「クラウド・サービス」を利用することに同意し、それらを遵守する一切の責任を負うものとします。

データの収集および処理の承認

「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」オファリング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」を操作する「対象参加者」および「クライアント・デバイス」から情報を収集します。「クラウド・サービス」は、一部の国または地域において、単独で、または組み合わせにより、「個人データ」とみなされる可能性がある情報を収集します。「個人データ」とは、IBM に提供され、お客様のために保管、処理、または転送される、名前、電子メール・アドレス、住所、または電話番号といった特定の個人を識別することができるあらゆる情報をいいます。

データの収集および処理の手法は、「クラウド・サービス」の機能を改善するために更新されることがあります。データの収集および処理の手順について十分な説明が記載された文書は、必要に応じて更新され、要請に基づきお客様に提供されます。お客様は、本「サービス記述書」の「海外への移転」および「データ・プライバシー」の項に従ってかかる情報を収集し、処理する権限を IBM に付与するものとします。

Trusteer Management Application (TMA) を含む IBM Trusteer オファリングの場合

TMA 管理者のために、ご契約企業から以下のデータが収集・保管されます。電子メール・アドレス (ログインとして)、ハッシュ化されたパスワード、名前、姓、役職、および部門。

IBM Trusteer Pinpoint の「クラウド・サービス」の場合

収集されたデータには、以下が含まれる場合があります。

- ユーザーまたはエンドポイントの ID (暗号化または不可逆的にハッシュ化された「ユーザー ID」、「永続的ユーザー ID (PUID)」、「Rapport エージェント・キー」、および「カスタマー・セッション ID」など)。
- 保護されたアプリケーションに関連するデータ (エンド・ユーザーのブラウザー、Web サイト・アクセスおよび閲覧履歴でレンダリングされたお客様のオンライン・バンキング・アプリケーションからの特定の属性/要素など)。
- インストール済みソフトウェア環境情報、ブラウザーとデバイスの属性や設定、およびブラウザー履歴の長さ。
- ハードウェア情報およびタイム・スタンプ。
- ブラウザー・ヘッダーおよび通信プロトコル・データ (ユーザー IP アドレス、Cookie、参照者ヘッダー、およびその他の HTTP ヘッダーなど)。
- マウス・ポインターの座標、クリック、スクロール・ホイールの動き (およびそれぞれの同等のもの)、ならびにタイム・スタンプといった、お客様のオンライン・バンキング・アプリケーションを操作する間の、エンド・ユーザーのマウスの動きに関するデータ。
- フィッシング・サイトやフィッシング・サイトに送信された情報。
- お客様の独自の選択による、取引データ (取引金額、取引通貨および宛先コード、不可逆的にハッシュ化された取引対象銀行の識別名、不可逆的にハッシュ化された取引対象口座の識別名、取引が新規支払先の場合にはバイナリー値、および取引日時) およびオプションのリスク・データ・スコア。
- お客様の独自の選択による、エンド・ユーザーが、ユーザー名、パスワード、およびその他のテキストを入力するために使用するキーボード上のタイピング・リズムおよびキー・ストローク・ファミリー・シーケンス (ただし、文字や数字、特殊文字そのものではなく、ユーザー名やパスワードを識別する能力を持たないもの)。

お客様は、IBM がお客様の正式な帳簿もしくは記録またはその両方を収集、保管、管理および保持しないことを了承し、これに同意します。

お客様が、IBM Trusteer Rapport for Remediation オファリングまたは一部の Pinpoint サポートに加入する場合、IBM は、疑われるマルウェアの感染を調査し、確認するために、Rapport の「アカウント・ホルダーのクライアント・ソフトウェア」を「対象参加者」のマシンにインストールすることを推奨する場合があります。Rapport オファリングの収集されたデータは以下に規定されています。

IBM Trusteer Rapport の「クラウド・サービス」(Pinpoint オファリングによる収集に関連して導入される場合は Rapport for Remediation または Rapport for Mitigation を含みます。) の場合

収集されたデータには、以下が含まれる場合があります。

- 「アカウント・ホルダー」がアクセスする Web サイトの URL およびインターネット・プロトコル (IP) アドレスのうち、IBM が詐欺的なもの、フィッシングまたは搾取的なものの可能性があると判断するもの。および、特定済みの脅威の特性に関する情報。
- 「アカウント・ホルダー」がアクセスする Web サイトの URL および IP アドレスのうち、お客様が制御し、「クラウド・サービス」によって保護されるもの (オンライン・バンキング・サイトなど)。「アカウント・ホルダー」の IP アドレス。
- ハードウェア ID、オペレーティング・システム、アプリケーション・ソフトウェア、周辺ハードウェア、セキュリティー構成、システム設定、およびエンドポイントのネットワーク接続、さらにはエンドポイントの ID、名前、使用パターンおよびその他の識別可能な情報。
- プログラムのインストールおよび運用に関連する情報、プログラムの ID、プログラムのバージョン、エンドポイントから生成されたセキュリティー・イベント、ならびにプログラムのエラーに関する情報。
- 使用に関する統計およびプログラムが検出した脅威に関する統計情報。ブラウザーの異常終了、感染日時、および特定済みの脅威や誤動作の特性に関する情報を含むログ・ファイル。
- お客様の関連情報 (「ご契約企業」とも呼ばれます。)。関係情報は、エンド・ユーザーがご契約企業の Web サイトから Rapport をダウンロードするか、特定のご契約企業を選択した Trusteer サポート・サイトから Rapport をダウンロードするか、またはご契約企業のバンキング・アプリケーションにログオンしたときに確立されます。エンド・ユーザーは、複数のご契約企業の関連情報を持つことができます。
- 暗号化された「ユーザー ID」のうち、「アカウント・ホルダー」がお客様と対話するために使用するもののコピー (任意)。
- クレジット・カード番号のうち、プログラムが当該サイトは危険であると判断したことをプログラムが「アカウント・ホルダー」に通知した後で「アカウント・ホルダー」がサイトに入力したものの暗号化されたコピー。
- エンドポイントからのファイルおよびその他の情報のうち、IBM セキュリティーの専門家がマルウェアやその他の悪意のある活動に関連している可能性があると疑っているもの、または一般的なプログラムの誤動作に関連する可能性があるもの。
- エンド・ユーザーが「サポート」に問い合わせる際の個人的な連絡先情報 (名前および電子メールを含みます)。

IBM Trusteer Mobile SDK オファリングおよび IBM Trusteer Mobile Browser の「クラウド・サービス」の場合

収集されたデータには、以下が含まれる場合があります。

- ユーザー ID (暗号化または不可逆的にハッシュ化された「ユーザー ID」)。
- デバイス情報 (IP アドレス、ハッシュ化されたデバイス ID、タイム・スタンプ、インストール済みパッケージの MD5 値、ならびにその他のデバイスのハードウェアおよびソフトウェアの情報)
- Mobile SDK または Mobile Browser のバージョンおよびインストール日。
- 保護されたアプリケーションへの訪問
- お客様の関連情報。
- デバイスのリスク・データ (マルウェアの存在、ルートを隠すもの、Wi-Fi 暗号化の状態、デバイスが改造されているか否かなど)
- 異常終了のスタック・トレース (アプリケーションが予期せず終了した場合)
- 電話を構成するデータ (機種、メーカーなど)

- X および Y 座標、タッチエリアおよびアクションの種類 (上下および移動) を含む、エンド・ユーザーのタッチスクリーン操作情報
- 動作センサーのデータ、電源/リソースの使用、接続設定、環境センサー (気温、光および気圧など) ならびに一般的なデバイス設定 (音量、呼び出し音、画面の明るさなど).

8.3 データ主体のインフォームド・コンセント

IBM Trusteer Pinpoint の「クラウド・サービス」および IBM Trusteer Mobile SDK の「クラウド・サービス」の場合

お客様は、「クラウド・サービス」の合法的な利用、および「クラウド・サービス」を介した IBM による情報の収集と処理を可能にするために必要な、十分なインフォームド・コンセント、許可、または使用権を既に取得しているか、または取得することに同意するものとします。

IBM Trusteer Rapport の「クラウド・サービス」(Pinpoint の「クラウド・サービス」による収集に関連して導入される場合は Rapport Remediation または Rapport for Mitigation を含みます。)、および IBM Trusteer Mobile Browser の「クラウド・サービス」の場合

お客様は、「クラウド・サービス」の合法的な利用、および「ソフトウェア使用許諾契約」(https://www.trusteer.com/support/end-user-license-agreement で入手可能) に記載された情報の収集と処理を可能にするために必要な、十分なインフォームド・コンセントを取得する権限を IBM に付与するものとします。お客様が、(IBM ではなく) 自らがエンド・ユーザーとの間で同意の意思表示に対応すると決めた場合、お客様は、「クラウド・サービス」の合法的な利用、およびお客様のデータ・プロセッサーとしての IBM による「Cloud Service」を介した情報の収集と処理を可能にするために必要な、十分なインフォームド・コンセント、許可、または使用権を既に取得しているか、または取得することに同意するものとします。

8.4 セキュリティー・データの使用

報告作業を含む「クラウド・サービス」の一部として、IBM は、「クラウド・サービス」から収集された情報を匿名化または集約したものを準備し、維持管理します (以下「セキュリティー・データ」といいます) 。「セキュリティー・データ」では、下記 (d) に定めるものを除いて、お客様、その「対象参加者」および個人を特定することはありません。お客様は、以下のみを目的として IBM が「セキュリティー・データ」を無期限で使用またはコピーできることに同意します。

a. 「セキュリティー・データ」の公表または配布 (サイバーセキュリティーに関連する集計または分析など)

b. 製品やサービスの開発または拡張

c. 社内で、または第三者と共に実施する調査

d. 確認済みの第三者の攻撃者情報の合法的な共有

8.5 海外への移転

お客様は、以下に挙げる欧州経済地域外の国および欧州委員会により十分なレベルのセキュリティーを実現しているとみなされる国 (アメリカ合衆国) に所在するプロセッサーおよびサブプロセッサーに対して、IBM が、関連法規および要件に基づいて、上記の「合法的使用および同意」の項で特定されたあらゆる「個人データ」を含む「コンテンツ」を国域を越えて処理できることに同意するものとします。

8.6 データ・プライバシー

お客様が、EU 加盟国、アイスランド、リヒテンシュタイン、ノルウェーまたはスイスにおいて、「個人データ」を「クラウド・サービス」に提供する場合、またはそれらの国に所在する「対象参加者」または「クライアント・デバイス」がお客様にある場合は、唯一のコントローラーとしてのお客様は、「個人データ」を処理するプロセッサー (かかる用語は、EU 指令 95/46/EC で定められています) として IBM を指名するものとします。IBM は、IBM が公表した「クラウド・サービス」の説明書に従って「クラウド・サービス」オファリングを提供するために必要な範囲でのみ、かかる「個人データ」を処理するものとし、お客様は、かかる処理がすべてお客様の指示に従っていることに同意するものとします。IBM が、処理ロケーションに、または「クラウド・サービス」の一部として「個人データ」を保護する方法に、重大な変更を加える場合、IBM は「Customer Portal」を介して相当の事前通知を行います。お客様は、

IBM がお客様に変更を通知した日から 30 日以内に IBM に対して書面にて通知することにより、影響を受けた「クラウド・サービス」の現在のサブスクリプション期間を終了させることができます。

当事者またはその関連会社は、選択条項を除いた EC Decision 2010/87/EU に従って、該当するそれぞれの役割において、修正が加えられていない EU 標準契約条項契約を個別に締結することができます。これらの契約に起因するすべての紛争または責任については、両当事者は、関連会社間の紛争であっても、本契約の条件に基づき、紛争または責任が両当事者間で生じた場合と同様に取り扱うものとします。

a. お客様は、プロビジョニング処理の間に判断されたとおり、ドイツのデータセンターを介して提供されたサービスについて、以下のプロセッサーおよびサブプロセッサーに対して、あらゆる「個人データ」を含む「コンテンツ」を国域を越えて処理できることに同意するものとします。

プロセッサーまたは サブプロセッサーの名称	役割 (データのプロセッサー またはサブプロセッサー)	所在地
IBM 契約事業体	プロセッサー	「取引文書」に記載
Amazon Web Services (ドイツ)	サブプロセッサー	ドイツ
IBM Ireland Ltd.	プロセッサー	アイルランド
IBM Israel Ltd.	プロセッサー	イスラエル

ドイツのデータセンターを通じて提供されるサービスに関して、一部のお客様サポート・サービスは、任意の EU 加盟国に所在する Trusteer の従業員によって提供される場合があります。

b. お客様は、プロビジョニング処理の間に判断されたとおり、日本のデータセンターを介して提供されたサービスについて、以下のプロセッサーおよびサブプロセッサーに対して、あらゆる「個人データ」を含む「コンテンツ」を国域を越えて処理できることに同意するものとします。

プロセッサーまたは サブプロセッサーの名称	役割 (データのプロセッサー またはサブプロセッサー)	所在地
IBM 契約事業体	プロセッサー	日本 (「取引文書」に記載のとおり)
Amazon Web Services (日本)	サブプロセッサー	日本
IBM Ireland Ltd.	プロセッサー	アイルランド
IBM Israel Ltd.	プロセッサー	イスラエル

c. お客様は、米国のデータセンターを介して提供されたサービスについて、以下のプロセッサーおよびサブプロセッサーに対して、あらゆる「個人データ」を含む「コンテンツ」を国域を越えて処理できることに同意するものとします。

プロセッサーまたは サブプロセッサーの名称	役割 (データのプロセッサー またはサブプロセッサー)	所在地
IBM 契約事業体	プロセッサー	「取引文書」に記載
Amazon Web Services LLC	サブプロセッサー	米国
IBM Ireland Ltd.	プロセッサー	アイルランド
IBM Israel Ltd.	プロセッサー	イスラエル
IBM Corp	プロセッサー	米国

d. 上記第 8.5.c 項「米国データセンター」に記載されたデータセンターを介して提供されたサービスについて、IBM は、プロビジョニング処理の間に判断されたとおり、以下の該当するサブプロセッサーのうち 1 つ以上を用いて処理することができます。

プロセッサーまたは サブプロセッサーの名称	役割 (データのプロセッサー またはサブプロセッサー)	所在地
Amazon Web Services (オーストラリア)	サブプロセッサー	オーストラリア
Amazon Web Services (シンガポール)	サブプロセッサー	シンガポール
Amazon Web Services (アイルランド)	サブプロセッサー	アイルランド

e. お客様は、IBM が、「Customer Portal」を通じた通知により、Amazon Web Services から IBM のデータセンターに処理を移行できることに同意します。さらに、IBM は、「Customer Portal」を通じた通知により、上記のサブプロセッサー一覧を変更することができます。

f. 「アカウント・ホルダー」のデータは、「アカウント・ホルダー」が最初に「アカウント・ホルダーのクライアント・ソフトウェア」をインストールした際のインストール元である地域で処理されます。つまり、「アカウント・ホルダー」のコンテンツが当初の地域およびお客様が同意した地域の両方で処理されることが、まれにあるということです。

g. お客様のサポート・データは、アイルランドに配置されている Salesforce.com クラウド・サーバーに保管されます。

h. 明確にするために付言すると、Trusteer Fraud Protection は統合ソリューションであるため、お客様がこれらの「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」に従って、お客様に残りの「クラウド・サービス」を提供するためにお客様のデータを保持することができます。

9. サービス・レベル・アグリーメント

IBM は、「PoE」に記載するとおり、「クラウド・サービス」に関して、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。) を提供します。「SLA」は保証ではありません。「SLA」はお客様にのみ提供され、実稼働環境における使用に対してのみ適用されます。

9.1 可用性クレジット

お客様は、「クラウド・サービス」の可用性に影響を及ぼした事象について最初に知り得たときから 24 時間以内に、IBM テクニカル・サポート・ヘルプデスクに対して「重要度 1」のサポート・チケットを記録するものとします。お客様は、あらゆる問題診断および解決に関して IBM を合理的な範囲で支援するものとします。

「SLA」の未達を申告するサポート・チケットは、契約月の末日から 3 営業日以内に提出するものとします。有効な「SLA」の申告に対する補償は、「クラウド・サービス」の実稼働システム処理が利用できない時間 (以下「ダウンタイム」といいます。) に基づいた「クラウド・サービス」の将来の請求に対するクレジットになります。「ダウンタイム」は、お客様が当該事象を報告した時点から「クラウド・サービス」が復元される時点までの間で計測され、次のものに関連する時間は含まれません。保守のための計画停止または発表された停止、IBM の支配の及ばない原因、お客様または第三者のコンテンツもしくはテクノロジーの問題または設計もしくは指示、サポート対象外のシステム構成およびプラットフォームまたはその他お客様による誤り、またはお客様に起因するセキュリティーに関する事故もしくはお客様によるセキュリティー・テスト。IBM は、下表のとおり、各契約月における「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。各契約月の補償の合計額は、「クラウド・サービス」に対する年額料金の 12 分の 1 の 10% を超えないものとします。

9.2 サービス・レベル

「契約月」における「クラウド・サービス」の可用性

「契約月」における可用性	補償 (申告の対象である「契約月」における 「月額サブスクリプション料金」* の割合)
< 99.5%	2%
< 98.0%	5%
< 96.0%	10%

*「クラウド・サービス」が IBM ビジネス・パートナーから取得されたものである場合、月額サブスクリプション料金は、申告の対象である「契約月」に対して有効な「クラウド・サービス」のその時点での最新の表示価格に基づいて計算され、それを 50% 割引した額となります。IBM は、直接お客様に払い戻します。

「サービス・レベル」および関連する「サービス・クレジット」は、「クラウド・サービス」単位および「クライアント・アプリケーション」単位で個別に測定されます。

「アプリケーション」の使用許諾に基づいて「クラウド・サービス」の SLA クレジットを算出する際、以下のガイドラインに基づいて「可用性」は算出されます。

- 各「アプリケーション」には、契約月の間にカウントされたセッション数量に基づいて割り当てられる加重シェアが設定されます。
- 「アプリケーション」当たりの各「クラウド・サービス」のダウンタイムは、契約月に対して別途集計されます。

以下は、1 か月分のアクティビティーおよび関連する加重の計算例です。 これは説明のみを目的としています。

個人向け アプリケーション	所定の契約月の セッション総数に 占める割合	契約月中の「合計 ダウンタイム」	加重処理後のダウンタイムの 分単位の時間数
個人向け アプリケーション A	40%	300 分	40% x 300 分 = 120 分
個人向け アプリケーション B	20%	250 分	20% x 250 分 = 50 分
個人向け アプリケーション C	40%	150 分	40% x 150 分 = 60
			加重処理後のダウンタイムの分単位の総時間数 = 230

「可用性」は、以下のとおり算出されます。契約月における分単位の総時間数から、契約月における加重処理後の「ダウンタイム」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。上記の加重例に基づくサンプルの計算は以下のとおりです。

30 日の「契約月」における合計 43,200 分 - 加重処理後の「ダウンタイム」230 分 = 42,970 分 合計 43,200 分	=「契約月」における 99.4% の可用性につき 2% の「可用性クレジット」

10. テクニカル・サポート

「クラウド・サービス」のテクニカル・サポートは、お客様およびその「対象参加者」に対して、その「クラウド・サービス」の利用を支援するために提供されます。

標準サポートは、すべてのオファリングのサブスクリプションに含まれています。Trusteer Rapport のアドオンである Trusteer Rapport Mandatory Service には、基本となる Trusteer Rapport のサブスクリプションに対するプレミアム・サポートの前提条件があります。

「クラウド・サービス」ごとに、プレミアム・サポートのサブスクリプションを追加料金で利用できます。ただし、IBM Trusteer Mobile SDK および IBM Trusteer Rapport Mandatory Service の各「クラウド・サービス」は除きます。IBM 営業担当員または IBM ビジネス・パートナーにお問い合わせください。

標準サポート

- 現地時間祝日を除く月曜日から金曜日の午前 9 時 - 午後 5 時のサポート
- お客様およびその「対象参加者」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-01.ibm.com/software/security/trusteer/support/.
- サポートのオプションおよび詳細については、以下の「SaaS サポート・ハンドブック」にアクセスしてください。http://www-01.ibm.com/software/support/handbook.html.

プレミアム・サポート

- 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「対象参加者」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-01.ibm.com/software/security/trusteer/support/.
- サポートのオプションおよび詳細については、以下の「SaaS サポート・ハンドブック」にアクセスしてください。http://www-01.ibm.com/software/support/handbook.html.

11. エンタイトルメントおよび課金情報

11.1 課金単位

「クラウド・サービス」は、「取引文書」に記載された課金単位に基づいて提供されます。

a. **「対象参加者」**は、「クラウド・サービス」を取得する際の課金単位です。「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各個人または法人は、「対象参加者」です。お客様の「取引文書」に定める課金期間中に、「クラウド・サービス」内で管理または追跡されるすべての「対象参加者」をカバーするために十分なエンタイトルメントを取得しなければならないものとします。

「クラウド・サービス」によって管理される各サービス提供プログラムは、個別に分析された後にまとめられます。複数のサービス提供プログラムの利用資格を有する個人または組織は、それぞれ独立してエンタイトルメントが必要になります。

かかる「IBM クラウド・サービス」のエンタイトルメントにおいて、「対象参加者」は、「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」の固有のログイン資格情報を有するお客様のエンド・ユーザーです。

b. **「クライアント・デバイス」**は、「クラウド・サービス」を取得する際の課金単位です。「クライアント・デバイス」とは、単一ユーザーのコンピューティング・デバイス、または特定用途のセンサー・デバイスもしくは遠隔測定デバイスのうち、一般にサーバーと呼ばれる (あるいはサーバーで管理される) 別のコンピューター・システムから、一連のコマンド、プロシージャー、もしくはアプリケーションを実行することを要求、それらを実行するために受領、またはかかるコンピュー

ター・システムにデータを提供するものをいいます。複数の「クライアント・デバイス」で 1 つの共通サーバーへのアクセスを共用することができます。「クライアント・デバイス」は、ユーザーが作業を実施できるように、何らかの処理機能を有するか、プログラムで制御することが可能な場合があります。お客様は、お客様の「取引文書」に定める課金期間中に「クラウド・サービス」を実行する、「クラウド・サービス」にデータを提供する、「クラウド・サービス」により提供されるサービスを利用する、または「クラウド・サービス」にアクセスするすべての「クライアント・デバイス」に対してエンタイトルメントを取得しなければならないものとします。

c. **「アプリケーション」**は、「クラウド・サービス」を取得する際の課金単位です。「アプリケーション」は、固有の名前が付けられたソフトウェア・プログラムです。お客様の「PoE」または「取引文書」に定める課金期間中にアクセスおよび利用することが可能な「アプリケーション」ごとに十分なエンタイトルメントを取得しなければならないものとします。

この「クラウド・サービス」において、1 つのアプリケーションとは、お客様の 1 つの「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」です。

d. **「エンゲージメント」**は、サービスを取得する際の課金単位です。「エンゲージメント」は、「クラウド・サービス」に関連するプロフェッショナル・サービス、研修サービスまたはその両方のサービスで構成されます。それぞれの「エンゲージメント」をカバーするのに十分なエンタイトルメントを取得しなければならないものとします。

11.2 1 か月に満たない期間の料金

「取引文書」に記載された 1 か月に満たない期間の料金は、按分にて算定される場合があります。

12. 遵守および監査

IBM Trusteer Fraud Protection の「クラウド・サービス」へのアクセスは、「取引文書」に定められた「アプリケーション」、「対象参加者」および「クライアント・デバイス」、またはそのいずれかの最大数に従うものとします。お客様は、「アプリケーション」、「対象参加者」および「クライアント・デバイス」、またはそのいずれかの数が「取引文書」に定められた最大数を超えないようにする責任を負うものとします。

「アプリケーション」、「対象参加者」および「クライアント・デバイス」、またはそのいずれかの最大数が遵守されていることを確認するために、監査が IBM によって実施される場合があります。

13. 期間および更新オプション

「クラウド・サービス」の期間は、「PoE」に記述されるとおり、「クラウド・サービス」へのお客様のアクセスについて、IBM がお客様に通知した日に開始します。「PoE」には、「クラウド・サービス」が自動的に更新されるか、継続利用ベースで続行されるか、期間満了時に終了するかが記載されます。

自動更新の場合には、お客様が期間満了日の少なくとも 90 日前までに書面により更新しないことを通知する場合を除き、「クラウド・サービス」は、「PoE」に定める期間につき自動更新されます。

継続利用の場合は、「クラウド・サービス」は、お客様が 90 日前までに書面により終了を通知するまで、月単位で継続利用することができます。「クラウド・サービス」は、かかる 90 日の期間後の暦月末日まで引き続き利用することができます。

14. イネーブリング・ソフトウェア

本「クラウド・サービス」には、「クラウド・サービス」期間にわたって、「クラウド・サービス」のお客様による使用に関連してのみ使用することのできるイネーブリング・ソフトウェアが含まれます。

15. IBM Trusteer の年間サブスクリプション料金の引き上げ

IBM は、「クラウド・サービス」のサブスクリプション料金を調整する権利を留保します。サブスクリプション料金の調整は、該当する「見積書」に記載されている価格とその期間に対して反映されます。12 か月に 1 回を限度に、IBM が決定する比率 (3% を超えない) で適用される追加のサブスクリプション料金の調整は、「クラウド・サービス」の期間が自動更新または継続使用を通じて延長されるときに適用される場合があります。これらの料金の調整により、お客様の「クラウド・サービス」のエンタイトルメントや「クラウド・サービス」の取得に用いられる課金単位が変更されることはありません。

「IBM ビジネス・パートナー」は IBM から独立した事業体であり、提供する製品、サービスに対する価格および条件を独自に決定します。