IBM Trusteer Pinpoint Detect

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 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. Trusteer Management Application (TMA) および Trustboard:

TMA は、お客様によるアラートの評価と分類が可能な Trusteer の従来の管理アプリケーションです。Trustboard は新しい管理アプリケーションで、その主な用途は調査になります。TMA と Trustboard は同時に使用できないため、どちらかを選択して使用してください。TMA および Trustboard 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 および Trustboard 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。IBM Trusteer Pinpoint Detect および IBM Trusteer Pinpoint Verify は、TMA および Trustboard のログインの一部として使用されます。

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、またはそれをテストもしくは使用するための、Web サイト上での導入用です。

「セッション」とは、お客様の「アプリケーション」(Web またはモバイル) と、1 つ以上のリアルタイムのリスク評価を生成する「クラウド・サービス」の間の対話をいいます。「セッション」は、対話の開始時から対話の終了時まで計測されます。対話の終了は、以下のいずれかのイベントが発生した時に記録されます。

- アプリケーションのログアウトという通常の方法で対話がリセットされる。
- ブラウザー、アプリケーション、またはタブがクローズされる。
- Cookie が削除される。
- タイムアウトになる。

「セッション」には、ログイン、閲覧、チェックアウト、支払い設定、その他お客様の「アプリケーション」で定められた活動など、任意の数の活動を含めることができます。本「クラウド・サービス」において、1 つの「コネクション」(下記に規定) は 1 つの「セッション」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 Pinpoint Detect Standard for Retail および IBM Trusteer Pinpoint Detect Standard for Business

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、「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、「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 (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「サービス」は、管理対象デバイスおよび管理対象外デバイスがもたらすリスクを評価するために、リモート従業員のアクセス用にも使用できます。

この「クラウド・サービス」には、プレミアム・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。

このサービスは、「適格参加者」100 人単位のパックまたは「コネクション」100 単位のパックで購入可能です。

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

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、統合が容易な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、「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。

このサービスには、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) が含まれます。このサービスには、導入サービスに対する最大 200 時間 (アプリケーションごと) の共有リソース、およびセットアップにおけるセキュリティー分析に対する最大 200 時間の共有リソース (アプリケーションごと) が含まれます。この継続的なサービスには、年間 20 時間 (アプリケーションごと) の導入保守、および年間 100 時間 (アプリケーションごと) のセキュリティー調査が含まれます。追加の取り組みは、追加料金の対象となります。

Pinpoint Detect では「モバイル」および Web の両チャネルから取引を取り込むことができます。「モバイル」の取引が含まれる場合には、Pinpoint by Connection を利用できます。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 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。

IBM Trusteer Pinpoint Detect Premium for Retail サービスおよび IBM Trusteer Pinpoint Detect Premium for Business サービスは、100 人単位の「適格参加者」のパックで、または IBM Trusteer Pinpoint Detect Premium については 100 単位の「コネクション」のパックで購入可能です。お客様が「コネクション」単位でサービスを購入することを選択した場合は、「追加アプリケーション」料金を 1 つ目のアプリケーションから適用可能です。

Pinpoint Detect Policy Manager:

Policy Manager は Pinpoint Detect Premium サービスに含まれ、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 Policy Manager により、(i) 不正な活動を検出するために実稼働環境ロジックを設計、テストおよび展開すること、(ii) レポートおよびダッシュボードを設計すること、ならびに (iii) セキュリティー・ポリシー、およびお客様の「アプリケーション」上の疑わしい活動を検出するポリシーを表示、構成、設定することができます。

Policy Manager 機能の有効化および追加のディープ・ダイブを必要とするサポートについては、コンサルティング・サービスが必要です。コンサルティング・サービスの詳細の概要は、作業指示書に別途記載されます。

Policy Manager を有効化した場合、IBM は、お客様のポリシーを調整し、ポリシー変更から生じる重大な問題を修正するサポートのために、お客様の環境へアクセスする権利を留保します。

お客様は、Policy Manager で公開されるデータを誤用から保護するものとします。

この Policy Manager の機能を有効化した場合、お客様は、資料の概要どおりに、ルール設定に関する IBM ガイドラインに従わなければなりません。お客様は、お客様がこれらの推奨事項に従わないことによって生じる可能性のある状況に対して、IBM が責任を負わないことを認めます。

この Policy Manager 機能のお客様による構成ミスが原因で生じる可能性のある安定度およびサービス低下またはそのいずれかに関する問題は、SLA 計算の「ダウンタイム」とはみなされません。

1.1.3 IBM Trusteer Pinpoint Detect for Connections

本「クラウド・サービス」は保護を提供し、アカウント乗っ取りの試みを検出することを目的とし、「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 (お客様のモバイル・アプリケーションのネイティブ・ブラウザーを介して) 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/信頼性評価スコアを提供します。このソリューションでは、エンド・ユーザーのデバイス、接続および振る舞いを分析するためのさまざまなリスク指標を使用し、ユーザーの履歴と比較して疑わしい使用を特定します。

本「クラウド・サービス」ではモバイルと Web の両チャネルから接続を取り込むことができます。IBM Trusteer Pinpoint Detect には、関連性がある場合、IBM Trusteer Mobile SDK の使用許諾が含まれます。

「クラウド・サービス」は年間 100 単位の「コネクション」のパックで購入可能です。

1.2 オプション・サービス

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

1.2.1 IBM Trusteer Pinpoint Detect Standard Application

「クライアント・アプリケーション」は、「Web アプリケーション」および「モバイル・アプリケーション」またはそのいずれかを指します。「Web アプリケーション」とは、ログイン画面または識別画面から、いくつかの Web ページを経由してお客様の「適格参加者」に提供され、Trusteer コンソール (Trusteer Management Application) で 1 つの「アプリケーション」として監視されるすべての機能をまとめて呼びます。「モバイル・アプリケーション」とは、ログイン画面または識別画面から、アプリケーション・ストア (ストア) からダウンロード可能な 1 つのソフトウェア・プログラムを経由してお客様の「適格参加者」に提供され、Trusteer コンソール (Trusteer Management Application) で 1 つの「アプリケーション」として監視されるすべての機能をまとめて呼びます。

IBM Trusteer Pinpoint の統合には、「アプリケーション」ごとに IBM Trusteer Pinpoint Application の使用許諾が必要です。

- IBM Trusteer Pinpoint Detect Standard の導入には、「アプリケーション」ごとに IBM Trusteer Pinpoint Detect Standard Application の使用許諾が必要です。

1.2.2 IBM Trusteer Pinpoint Detect Premium Application

「クライアント・アプリケーション」は、「Web アプリケーション」および「モバイル・アプリケーション」またはそのいずれかを指します。「Web アプリケーション」とは、ログイン画面または識別画面から、いくつかの Web ページを経由してお客様の「適格参加者」に提供され、Trusteer コンソール (Trusteer Management Application) で 1 つの「アプリケーション」として監視されるすべての機能をまとめて呼びます。「モバイル・アプリケーション」とは、ログイン画面または識別画面から、アプリケーション・ストア (ストア) からダウンロード可能な 1 つのソフトウェア・プログラムを経由してお客様の「適格参加者」に提供され、Trusteer コンソール (Trusteer Management Application) で 1 つの「アプリケーション」として監視されるすべての機能をまとめて呼びます。

このサービスには、導入サービスに対する最大 200 時間 (アプリケーションごと) の共有リソース、およびセットアップにおけるセキュリティー分析に対する最大 200 時間の共有リソース (アプリケーションごと) が含まれます。この継続的なサービスには、年間 20 時間 (アプリケーションごと) の導入保守、および年間 100 時間 (アプリケーションごと) のセキュリティー調査が含まれます。

- IBM Trusteer Pinpoint Premium の導入には、「アプリケーション」ごとに IBM Trusteer Pinpoint Detect Premium Application の使用許諾が必要です。

1.2.3 IBM Trusteer New Account Fraud for Retail または IBM Trusteer New Account Fraud for Business

Pinpoint の加入者が利用できるこのサービスは、異常を検出し、疑わしいアクティビティーにフラグを立て、新規の口座作成処理の初期の段階でアラートを生成するように設計されています。本サービスは、TMA で入手できる利用レポートにより、新規の口座が、違法送金の口座かまたは詐欺に利用される可能性があるという警告サインを早期に発するために、詐欺事後口座および新しい口座プロファイルに関連する新しいアクティビティーを特定するため、新規口座をモニターします。

IBM Trusteer New Account Fraud for Retail および IBM Trusteer New Account Fraud for Business は、「API 呼び出し」10 回単位のパックで入手することができます。

1.2.4 IBM Trusteer Digital Content Pack for Retail および IBM Trusteer Digital Content Pack for Business またはそのいずれか

IBM Trusteer Digital Content Pack は、セキュリティー・アナリストが、進化する脅威に対応するために特定のモデルの作成および修正をサポートすると同時に、新たな不正対策モデルを統合できるようにします。この製品は、このソリューションの重要な追加部分として購入可能な広範囲にわたるルール、洞察、およびポリシーで構成されています。Digital Content Pack は、Trusteer のデジタル不正防止に関する各種機能および IBM Safer Payments のキャッシュレス支払いチャネル間の統合をさらに強化するのに役立ちます。Digital Content Pack は組み込まれているルールおよび個別のビジネス・ロジックを活用して、銀行やその他の金融機関が既存の不正検出機能や不正防止機能をさらに強化できるようにします。

IBM Trusteer Digital Content Pack for Retail は、「適格参加者」100 人単位のパックで利用可能です。IBM Trusteer Digital Content Pack for Business は、「適格参加者」10 人単位のパックで利用可能です。

Digital Content Pack と、Pinpoint Detect および IBM Safer Payments との統合、ならびに相当の注意を必要とするサポート・サービスについては、コンサルティング・サービスが必要です。コンサルティング・サービスは、別個の作業指示書に従って別途ご購入いただきます。

1.2.5 IBM Trusteer Pinpoint Malware Detection

IBM Trusteer Pinpoint Malware Detection II の「クラウド・サービス」でマルウェアを検出した場合、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 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 の「クラウド・サービス」に結び付けてしまうような影響を「適格参加者」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)。

1.2.6 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「適格参加者」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 100,000 の「個人向け適格参加者」(100 単位の「個人向け適格参加者」が 1,000 パック) または 10,000 の「法人向け適格参加者」(10 単位の「法人向け適格参加者」が 1,000 パック) を最低数量として提供されます。

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。

1.2.7 IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail および IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail、ならびに IBM Pinpoint Trusteer Pinpoint Malware Detection Standard Edition II for Business および IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business に対するオプションの追加のクラウド・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 II for Retail または IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail の前提条件があります。
- 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 II for Business または IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business の前提条件があります。

1.2.8 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

TMA と Trustboard は同時に使用できないため、どちらかを選択して使用してください。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「適格参加者」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 または Trustboard のどちらか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。

1.2.9 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

   TMA と Trustboard は同時に使用できないため、どちらかを選択して使用してください。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「適格参加者」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 または Trustboard のどちらか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。

1.2.10 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「適格参加者」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 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「適格参加者」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「適格参加者」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「適格参加者」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「適格参加者」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。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。

1.2.11 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 Retail または IBM Trusteer Pinpoint Malware Detection Advanced Edition 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」の導入には、IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail の使用許諾が必要です。
- 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、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」の導入には、IBM Trusteer Pinpoint Malware Detection Additional Applications for Business の使用許諾が必要です。

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

- IBM Trusteer Rapport for Mitigation for Retail 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「適格参加者」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「適格参加者」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「適格参加者」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「適格参加者」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「適格参加者」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。
- IBM Trusteer Rapport for Mitigation for Business 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「法人向けアプリケーション」にアクセスするお客様の「適格参加者」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「法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「法人向けアプリケーション」にアクセスする「適格参加者」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 Business は、かかる感染した「適格参加者」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「適格参加者」が EULA を受諾し、お客様の「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「適格参加者」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。

1.2.13 IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail および IBM Trusteer Pinpoint Detect Standard Additional Applications for Business

- IBM Trusteer Pinpoint Detect Standard 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」の導入には、IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail の使用許諾が必要です。

- IBM Trusteer Pinpoint Detect Standard 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」の導入には、IBM Trusteer Pinpoint Detect Standard Additional Applications for Business の使用許諾が必要です。

1.2.14 IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail および IBM Trusteer Pinpoint Detect Premium Additional Applications for Business

このサービスには、導入サービスに対する最大 200 時間 (アプリケーションごと) の共有リソース、およびセットアップにおけるセキュリティー分析に対する最大 200 時間の共有リソース (アプリケーションごと) が含まれます。この継続的なサービスには、年間 20 時間 (アプリケーションごと) の導入保守、および年間 100 時間 (アプリケーションごと) のセキュリティー調査が含まれます。

- IBM Trusteer Pinpoint Premium 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」の導入には、IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail の使用許諾が必要です。
- IBM Trusteer Pinpoint Premium 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」の導入には、IBM Trusteer Pinpoint Detect Premium Additional Applications for Business の使用許諾が必要です。

1.2.15 IBM Trusteer Pinpoint Detect Standard for Retail Premium Support および IBM Trusteer Pinpoint Detect Standard for Business Premium Support

Pinpoint Detect Standard の「クラウド・サービス」を購入するお客様は、Premium Support サービスを購入できます。Premium Support のサービスの適用範囲は、以下の第 4 条に記載されています。

1.2.16 IBM Trusteer Mobile Carrier Intelligence for Pinpoint Detect

お客様は、本「クラウド・サービス」に申し込む前に、IBM Trusteer Pinpoint Detect 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。

本「クラウド・サービス」は、これらの「クラウド・サービス」のいずれかに提供される携帯電話番号に関する追加の情報およびコンテキストを提供することにより、IBM Trusteer Pinpoint Detect を拡張するもので、任意のセッションに関する不正のリスクを判断できるようにします。お客様は、所定の携帯電話番号に関する特徴 (その番号に関連するキャリア情報など) を把握するために「クラウド・サービス」への照会を実行できます。

携帯電話番号に関して本「クラウド・サービス」で提供されるデータ (以下「モバイル・インテリジェンス」といいます。) は、お客様の内部でのみ使用可能であり、30 日間限定で保持できます。お客様が、かかる期間の経過後に同一の携帯番号に関する「モバイル・インテリジェンス」を取得するには、当該番号に関して「クラウド・サービス」の照会を再実行する必要があり、前回の照会で受け取った「モバイル・インテリジェンス」をそのまま再使用してはなりません。お客様は、上記で認められている場合を除き、データ・マイニングの全部または一部に関連して、および一部を保存する目的で、当該「モバイル・インテリジェンス」を保存 (キャッシュ)、再使用、使用してはなりません。

1.3 アクセラレーション・サービス

1.3.1 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。

1.3.2 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 II 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。

IBM Trusteer Pinpoint Malware Detection Additional Applications。IBM Trusteer Pinpoint Malware Detection II Standard Edition または IBM Trusteer Pinpoint Malware Detection II Advanced Edition については、1 つ目の「アプリケーション」以外の追加の「アプリケーション」上での導入には、IBM Trusteer Pinpoint Malware Detection Additional Applications の使用許諾が必要です。

1.3.3 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。

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。

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 Mobile SDK

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

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。
- 「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。
- 「API 呼び出し」は、プログラマブル・インターフェースによる「クラウド・サービス」の呼び出しです。

- 「コネクション」とは、「クラウド・サービス」に対して提供されたまたは提供されている、データベース、アプリケーション、サーバー、またはその他のタイプのデバイスのリンクまたは関連付けです。

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 の「クラウド・サービス」(Pinpoint の「クラウド・サービス」に関連して導入される場合、Rapport Remediation または Rapport for Mitigation を含みます。) の場合: 別途の合意がある場合を除いて、お客様が独自に設定した処理の基準に従って、お客様は、IBM が「クラウド・サービス」を提供するために必要な情報を収集および処理することができるように、「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 Rapport 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、(1) 関連データが、IBM の第三者の復処理者としての 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、また (2) Mobile Carrier Intelligence プロバイダーにデータを送信することを選択したお客様の場合は、「個人データ」が「データ・シート」に記載された該当する第三者の復処理者の所在国でホストおよび処理される場合があります。「データ・シート」の相反する規定にかかわらず、直前の段落の第 2 項に記載されている第三者の復処理者は、ISO 27001 または SOC2 に準拠していない場合があります。

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 (IBM のお客様、「関連顧客」など) 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」のデータは上記の第 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 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「適格参加者」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)。

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。かかるデータには、特定の個人を識別したり、特定の個人に結びつけることができる情報が含まれていてはなりません。導入の一部として IBM に提供されるデータに関するガイドラインの詳細は、お客様に提供される Trusteer の「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。