# 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。

### Pinpoint Assure クラウド・サービス:

- IBM Trusteer Pinpoint Assure
- IBM Trusteer Pinpoint Assure Application
- IBM Trusteer Mobile Carrier Intelligence

### Rapport クラウド・サービス:

- IBM Trusteer Rapport for Business Premium Support
- 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 Standard Edition for Business Premium Support
- IBM Trusteer Pinpoint Malware Detection Standard Edition for Retail Premium Support
- IBM Trusteer Pinpoint Malware Detection Advanced Edition for Business Premium Support
- IBM Trusteer Pinpoint Malware Detection Advanced Edition for Retail Premium Support
- IBM Trusteer Rapport Remediation for Retail
- IBM Trusteer Rapport Remediation for Retail Premium Support
- IBM Trusteer Rapport Remediation for Business
- IBM Trusteer Rapport Remediation for Business Premium Support
- IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail
- IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business

- IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail
- IBM Trusteer Pinpoint Malware Detection Advanced Edition II 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 Detect Standard for Retail
- IBM Trusteer Pinpoint Detect Premium for Retail
- 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 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 Redeployment
- IBM Trusteer Pinpoint Detect Premium Redeployment
- IBM Trusteer Pinpoint Detect Standard for Retail Premium Support
- IBM Trusteer Digital Content Pack for Retail
- IBM Trusteer Digital Content Pack for Business
- IBM Trusteer New Account Fraud for Business
- IBM Trusteer New Account Fraud for Retail
- IBM Trusteer Project Management and Consultancy Services
- IBM Trusteer Security Research Consultancy Services
- IBM Trusteer Training Services
- IBM Trusteer Pinpoint Detect Standard Application
- IBM Trusteer Pinpoint Detect Premium Application
- IBM Trusteer Pinpoint Detect Standard
- IBM Trusteer Pinpoint Detect Premium
- IBM Trusteer Mobile Carrier Intelligence for Pinpoint Detect
- IBM Trusteer Pinpoint Verify

**Mobile クラウド・サービス:**

- IBM Trusteer Mobile SDK for Business
- IBM Trusteer Mobile SDK for Retail

## 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 II for Business
- IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business
- IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business
- IBM Trusteer Pinpoint Detect Standard for Business
- IBM Trusteer Pinpoint Detect Premium for Business
- IBM Trusteer Digital Content Pack for Business
- IBM Trusteer New Account Fraud for Business
- IBM Trusteer Mobile SDK for Business

### 1.1.2 個人向けのクラウド・サービス

- IBM Trusteer Rapport II for Retail
- IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail
- IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail
- IBM Trusteer Pinpoint Detect Standard for Retail
- IBM Trusteer Pinpoint Detect Premium for Retail
- IBM Trusteer Digital Content Pack for Retail
- IBM Trusteer New Account Fraud for Retail
- IBM Trusteer Mobile SDK 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 Additional Cloud Services for IBM Trusteer Rapport II

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。

### 1.1.4 IBM Trusteer Pinpoint Malware Detection II に対する追加の IBM クラウド・サービス

a. IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business または IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business に対する追加のクラウド・サービス

- IBM Trusteer Rapport Remediation for Business
- IBM Trusteer Pinpoint Malware Detection Additional Applications for Business

b. IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail または IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail に対する追加のクラウド・サービス

- 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 II for Business または 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 Detect Standard および IBM Trusteer Pinpoint Detect Premium、ならびに IBM Trusteer Pinpoint Detect Standard for Retail および IBM Trusteer Pinpoint Detect Premium for Retail、ならびに IBM Trusteer Pinpoint Detect Standard for Business および IBM Trusteer Pinpoint Detect Premium for Business に対する追加のクラウド・サービス

a. IBM Trusteer Detect Standard for Business および IBM Trusteer Pinpoint Detect Premium for Business 向けに提供されている追加のクラウド・サービス

- IBM Trusteer Pinpoint Detect Standard Additional Applications for Business
- IBM Trusteer Pinpoint Detect Premium Additional Applications for Business
- IBM Trusteer Digital Content Pack for Business
- IBM Trusteer New Account Fraud for Business

b. IBM Trusteer Detect Standard for Retail および IBM Trusteer Pinpoint Detect Premium for Retail 向けに提供されている追加のクラウド・サービス

- IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail
- IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail
- IBM Trusteer Digital Content Pack for Retail
- IBM Trusteer New Account Fraud for Retail

c. IBM Trusteer Pinpoint Detect Standard および IBM Trusteer Pinpoint Premium 向けに提供されている追加のクラウド・サービス

- IBM Trusteer Pinpoint Detect Standard Application
- IBM Trusteer Pinpoint Detect Premium Application

d. IBM Trusteer Pinpoint Detect Premium に対して利用可能な追加のクラウド・サービス

- IBM Trusteer Pinpoint Verify

IBM Trusteer Pinpoint Detect Standard もしくは IBM Trusteer Pinpoint Detect Premium、または IBM Trusteer Pinpoint Detect Standard for Retail もしくは IBM Trusteer Pinpoint Detect Premium for Retail、または IBM Trusteer Pinpoint Detect Standard for Business もしくは IBM Trusteer Pinpoint Detect Premium for Business のサブスクリプションは、本条項に記載されている追加の関連する「クラウド・サービス」の前提条件です。

### 1.1.6 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、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。

## 1.3 IBM Trusteer Rapport のクラウド・サービス

### 1.3.1 IBM Trusteer Rapport II for Retail および IBM Trusteer Rapport II for Business

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。) 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、「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」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「適格参加者」に無償で使用許諾されており、「適格参加者」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「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 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。「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。

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。

### 1.3.2 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。

### 1.3.3 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。

### 1.3.4 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。

### 1.3.5 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 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。

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。

### 1.3.6 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。

### 1.3.7 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。

## 1.4 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。

### 1.4.1 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)。

### 1.4.2 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。

### 1.4.3 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。

### 1.4.4 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。

### 1.4.5 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。

### 1.4.6 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。

## 1.5 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「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。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「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)。

### 1.5.1 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「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。Premium サポートについて、お客様は Pinpoint Standard Premium Support 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。

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。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。

### 1.5.2 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。

### 1.5.3 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 または IBM Trusteer Pinpoint Detect Standard に対する使用許諾が前提条件となります。

### 1.5.4 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。

### 1.5.5 IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail および IBM Trusteer Pinpoint Detect Standard Additional Applications for Business ならびに 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 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。
- 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。

### 1.5.6 IBM Trusteer Pinpoint Detect Standard Application および IBM Trusteer Pinpoint Detect Premium Application

本サービスは Web および「モバイル」の各チャネルに適用されます。

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。

- 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。
- 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。

### 1.5.7 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。

### 1.5.8 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。

### 1.5.9 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固別のビジネス・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。

### 1.5.10 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。

### 1.5.11 IBM Trusteer Pinpoint Verify

お客様は、本「クラウド・サービス」のサブスクリプション前に、IBM Trusteer Pinpoint Detect Premium 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、デジタル・サービスへのアクセス時にユーザーの ID を検証する目的で、二要素認証をユーザーに要求する機能を提供します。Pinpoint Detect Premium では、保護されたアプリケーションに対する二要素認証を提供するために、このサービスを使用できます。二要素認証をユーザーに要求するタイミングは、保護されたアプリケーションによって決定され、Pinpoint Detect Premium プラットフォームにより返される推奨事項、または保護されたアプリケーションにより定義されるその他のポリシーに基づくことができます。

## 1.6 IBM Trusteer Pinpoint Assure

このサービスでは、疑わしいアクティビティーにフラグが立てられ、新規口座の作成/登録プロセス時にはアラートが生成されます。このサービスは、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、詐欺に関連するアクティビティーを特定するため、口座登録プロセスをモニターします。

IBM Trusteer Pinpoint Assure は「コネクション」100 単位のパックで入手することができます。

### 1.6.1 IBM Trusteer Pinpoint Assure のオプション・サービス

### 1.6.2 IBM Trusteer Pinpoint Assure Application

IBM Trusteer Pinpoint Assure について、「アプリケーション」上での導入には、IBM Trusteer Pinpoint Assure Application の使用許諾が必要です。

IBM Trusteer Pinpoint Assure はアプリケーション単位で購入できます。

### 1.6.3 IBM Trusteer Mobile Carrier Intelligence for Pinpoint Detect および IBM Trusteer Mobile Carrier Intelligence for Pinpoint Detect

お客様は、本「クラウド・サービス」のサブスクリプション前に、IBM Trusteer Pinpoint Assure または IBM Trusteer Pinpoint Detect のいずれか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 Assure および IBM Trusteer Pinpoint Detect を拡張するもので、所定のセッションに関する不正のリスクを判断するのを手助けします。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。

## 1.7 IBM Trusteer Remotely Delivered Services

IBM Trusteer Remotely Delivered Services は、Pinpoint Detect Premium および Pinpoint Assure の「クラウド・サービス」に対するオプションのアドオンとして利用できます。

### 1.7.1 IBM Trusteer Project Management and Consultancy Services

このサービスでは、200 時間のコンサルティング・サービスを提供します。このサービスの間、IBM は以下の一部または全部のサービスを実行します。

a. 初期セットアップ・サービス: 頻繁に開かれる定期会議、プロジェクト管理サービス

b. 「ポリシー・マネージャー」: 継続的サポート

このオファリングは「エンゲージメント」単位にて購入できます。

### 1.7.2 IBM Trusteer Security Research Consultancy Services

このコンサルティング・サービスには、定義されたソリューションおよびプレミアム・サポート (該当する場合) に加えて追加のサービスを提供することを目的とした、最大 200 時間のセキュリティー分析用共有リソースが含まれるほか、以下が含まれます。

a. 不正に関する調査の拡張: 週次の会議および研修。

b. 優先度の高いお客様のリリース・サポート

c. 現行のカスタマイズされたルールに関する調査およびサポート

このオファリングは「エンゲージメント」単位にて購入できます。

### 1.7.3 IBM Trusteer Training Services

このコンサルティング・サービスは、定義されたソリューションおよびプレミアム・サポート (該当する場合) に加えて追加のサービスを提供するよう設計されたもので、お客様の従業員を対象とする Trusteer ポートフォリオの研修サービスを含みます。

このオファリングは「エンゲージメント」単位にて購入できます。

## 1.8 IBM Trusteer Mobile のクラウド・サービス

### 1.8.1 IBM Trusteer Mobile SDK for Business および IBM Trusteer Mobile SDK for Retail

IBM Trusteer Mobile SDK の「クラウド・サービス」は、お客様が申し込んでいる「クラウド・サービス」の範囲、デバイスのリスク評価、およびファー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、「適格参加者」100 人単位または「クライアント・デバイス」100 個単位のパックで入手可能です。また IBM Trusteer Mobile SDK for Business は、「適格参加者」10 人単位または「クライアント・デバイス」10 個単位のパックで入手可能です。

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

お客様は、以下を行うことができます。

a. 「お客様統合モバイル・アプリ」の開発のみを目的として、社内で IBM Trusteer Mobile SDK を使用すること。

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

c. 「適格参加者」のモバイル・デバイス上または「クライアント・デバイス」ホルダー上にダウンロードするために「再配布可能コード」を促進して配布すること。ただし、以下を条件とします。

   - 「本契約」で明示的に許可されている場合を除き、お客様は以下を行うことができません。(1) SDK を使用、コピー、修正、配布すること、(2) 強制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 Security Mobile SDK に含まれるモバイル・ツールを使用して作成されたアプリケーションまたはアウトプットが、特定のモバイル・オペレーティング・システム・プラットフォームもしくはモバイル・デバイスで機能すること、それらと相互運用すること、それらと互換性があることを保証しません。

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

## 2. コンテンツおよびデータ保護

「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」) には、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関する仕様に関する、「クラウド・サービス」に固有の情報が記載されています。「クラウド・サービス」およびデータ保護機能に関する詳細または説明および条件 (お客様の責任を含みます。) がある場合には、本条に記載されます。お客様が選択したオプションにより、お客様による「クラウド・サービス」の使用に適用される「データ・シート」が複数ある場合があります。「データ・シート」は英語のみの提供となります (現地言語での提供はありません)。現地の法律または慣習にかかわらず、両当事者は、英語を理解していること、および「クラウド・サービス」の取得および使用に関して英語が適切な言語であることに同意します。以下の「データ・シート」が「クラウド・サービス」およびその利用可能なオプションに適用されます。お客様は、i) IBM が、IBM の裁量により、「データ・シート」を随時変更することができ、かつ ii) かかる変更された内容が変更前の内容に置き換わることを承諾します。「データ・シート」に対する変更は、i) 既定の義務の改善もしくは明確化、ii) 最新の採用された基準および適用法への整合の維持、もしくは iii) 追加義務の規定のいずれかを行うことを意図しています。「データ・

シート」を変更しないことは、「クラウド・サービス」のデータ保護を著しく低下させることになります。

適用される「データ・シート」へのリンク:

**IBM Trusteer Mobile SDK**

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

**IBM Trusteer Mobile Secure Browser**

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=1402492579396

**IBM Trusteer Pinpoint Assure**

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

**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 Rapport**

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

**IBM Trusteer Pinpoint Verify**

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=735E5650E26711E69CCD7F0385C6524D

(IBM Cloud Identity Verify データ・シートは IBM Trusteer Pinpoint Verify を反映しています。)

お客様は、利用可能な「クラウド・サービス」に対してデータ保護機能を注文し、有効化し、または使用するために必要な措置を講じる責任を負うものとし、お客様が当該措置を講じなかった場合 (「コンテンツ」に関するデータ保護またはその他の法的要件を満たさないことも含みます。)、「クラウド・サービス」の使用に責任を負うものとします。

EU 一般データ保護規則 (EU/2016/679) (GDPR) が「コンテンツ」に含まれる個人データに適用される場合に、その適用範囲に限り、http://ibm.com/dpa にある IBM の「データ処理補足契約書」(DPA) および「DPA 別表」が適用され、本契約の一部として参照されます。本「クラウド・サービス」に適用される「データ・シート」は「DPA 別表」の位置づけです。DPA が適用される場合、「復処理者」の変更の通知を提供する IBM の義務およびかかる変更に異議を申し立てるお客様の権利は、DPA に規定されるとおりに適用されます。

## 2.1 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は 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://www.trusteer.com/support/end-user-license-agreement に掲載) を IBM が提供することを許可します。

## 2.2 データの利用

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 (「洞察」) や、お客様を特定できる結果を利用したり開示したりしません。ただし、IBM は、個人を特定する情報を削除し、追加情報を用いなければいかなる個人情報も特定の個人に結びつけることができないようにしたうえで、「クラウド・サービス」を提供する過程で、「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。) を使用できます。IBM は、研究、テスト、およびオファリング開発の目的でのみ、このデータを使用します。

## 2.3 データの処理および保存

### 2.3.1 処理ロケーションに関する追加情報

Trusteer Pinpoint Verify サービスについて、すべてのホスティングおよび処理の場所は関連する「データ・シート」に記載されています。

ドイツのデータセンターを通じて提供されるすべてのその他のサービスに関して、IBM は、「個人データ」の処理を、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、ならびに IBM の「第三者復処理者」向けの該当するデータ・シートに記載された追加の各国。

日本のデータセンターを通じて提供されるすべてのその他のサービスに関して、IBM は、「個人データ」の処理を、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、ならびに IBM の「第三者復処理者」向けの該当するデータ・シートに記載された追加の各国。

米国のデータセンターを通じて提供されるすべてのその他のサービスに関して、IBM は、「個人データ」の処理を、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、ならびに IBM の「第三者復処理者」向けの該当するデータ・シートに記載された追加の各国。

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。

### 2.3.2 アカウント・ホルダーのデータ

「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。

### 2.3.3 統合ソリューション

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。

# 3. 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。

## 3.1 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。

## 3.2 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<br>(申告の対象である「契約月」における<br>「月額サブスクリプション料金」* の割合) |
|---|---|
| < 99.9% | 2% |
| < 99.0% | 5% |
| < 95.0% | 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」および関連する補償クレジットは、「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<br>アプリケーション | 所定の契約月の<br>セッション総数に<br>占める割合 | 契約月中の<br>「合計ダウンタイム」 | 加重処理後のダウンタイムの<br>分単位の時間数 |
|---|---|---|---|
| 個人向け<br>アプリケーション A | 40% | 300 分 | 40% x 300 分 = 120 分 |
| 個人向け<br>アプリケーション B | 20% | 250 分 | 20% x 250 分 = 50 分 |
| 個人向け<br>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<br>- 加重処理後の「ダウンタイム」230 分<br>= 42,970 分<br>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」 |

## 4. 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「適格参加者」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、Premium Support 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 の「クラウド・サービス」**および **IBM Trusteer Rapport Mandatory Service の「クラウド・サービス」**、**IBM Trusteer New Account Fraud**、**IBM Trusteer Pinpoint Assure**、**IBM Trusteer Digital Content Pack** および **IBM Trusteer Mobile Carrier Intelligence** 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「適格参加者」は、IBM SaaS サポート・ガイド (https://www.ibm.com/software/support/saas_support_guide.html に掲載) 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

**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「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/
- サポートのオプションおよび詳細については、以下に掲載されている IBM の SaaS サポート・ガイドにアクセスしてください。https://www.ibm.com/software/support/saas_support_guide.html

## 5. エンタイトルメントおよび課金情報

### 5.1 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。

- 「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。
- 「適格参加者」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、「適格参加者」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「適格参加者」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、「適格参加者」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。

- 「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。
- 「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。

  本「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。
- 「API 呼び出し」は、「クラウド・サービス」を取得する際の課金単位です。「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。お客様の「PoE」または「取引文書」に定める課金期間中の「API 呼び出し」の総数 (10 単位で切り上げ) 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。
- 「コネクション」は、「クラウド・サービス」を取得する際の課金単位です。「コネクション」とは、「クラウド・サービス」に対するデータベース、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。お客様の「PoE」または「取引文書」に定める課金期間中に「クラウド・サービス」に接続しているか、または接続する「コネクション」の総数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。

  本「クラウド・サービス」において、1 つの「コネクション」とは、お客様の「アプリケーション」における 1 回のセッションまたは 1 つのフローです。

## 5.2 超過料金

課金期間中の「クラウド・サービス」の実際の利用が、「PoE」に記載されたエンタイトルメントを超える場合には、かかる超過が生じた月の翌月に、「取引文書」に記載された料金で超過料金が請求されます。

## 5.3 請求頻度

選択された請求頻度に基づき、IBM は請求頻度期間の開始時点で支払い期日の到来している料金をお客様に請求します。ただし、後払いとして請求される種類の使用料金および超過料金は除きます。

## 6. 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」が自動更新されるのか、連続的な使用に応じて継続されるのか、または契約期間の最終日をもって終了するのかが記載されます。

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。更新には、見積書に記載のとおり年次の値上げが適用されます。「クラウド・サービス」の営業活動終了に関する IBM 通知を受領後に自動更新が行われた場合、当該更新期間は、現在の更新期間の終了日または発表された営業活動終了日のいずれか早期に到来する日に終了します。

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。

## 7. 追加条件

### 7.1 共通事項

お客様は、IBM が広報活動またはマーケティングのコミュニケーションにおいて、お客様を「クラウド・サービス」の利用者として公に言及できることに同意します。

お客様は、「クラウド・サービス」を、単体または他のサービスもしくは製品と組み合わせて、高リスク活動、即ち核施設、公共交通システム、航空管制システム、自動車制御システム、兵器システム、または航空機の航行もしくは通信の設計、構築、管理、もしくは保守、または「クラウド・サービス」の障害が生命の危険や重大な人身傷害を引き起こすおそれがあるその他のいかなる活動のサポートのためにも使用しないものとします。

### 7.2 イネーブリング・ソフトウェア

「クラウド・サービス」を使用するには、お客様がご自身のシステムにイネーブリング・ソフトウェアをダウンロードする必要があります。イネーブリング・ソフトウェアにより、「クラウド・サービス」の使用が促進されます。お客様は、「クラウド・サービス」の利用に関連してのみ、イネーブリング・ソフトウェアを使用することができます。イネーブリング・ソフトウェアは現状のまま提供されます。

### 7.3 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。