IBM Security Trusteer Fraud Protection

ご利用条件 (以下、「ToU」といいます。) は、本「IBM ご利用条件 - SaaS 特定オファリング条件」(以下、「SaaS 特定オファリング条件」といいます。)、および以下の Web サイトでご覧いただける「IBM ご利用条件 - 一般条件」(以下、「一般条件」といいます。) という表題の文書で構成されています (URL:http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/)。

「SaaS 特定オファリング条件」と「一般条件」の規定に矛盾がある場合は、「SaaS 特定オファリング条件」が優先して適用されるものとします。「IBM SaaS」の注文、そのアクセスまたは利用により、お客様は本「ToU」に同意したものとみなされます。

「ToU」には、該当する「IBM パスポート・アドバンテージのご契約条件」、「IBM パスポート・アドバンテージ・エクスプレスのご契約条件」、または「IBM SaaS 特定オファリングのご契約条件」(以下、「本契約」といいます。) が適用され、これらと「ToU」と合わせて完全な合意として成立します。

1. IBM SaaS

以下の「IBM SaaS」オファリングは、これらの「SaaS 特定オファリング条件」の対象です。

1.1 Rapport IBM SaaS オファリング

- IBM Security Trusteer Rapport for Business
- IBM Security Trusteer Rapport for Business Premium Support
- IBM Security Trusteer Rapport for Retail
- IBM Security Trusteer Rapport for Retail Premium Support
- IBM Security Trusteer Rapport Fraud Feeds for Business
- IBM Security Trusteer Rapport Fraud Feeds for Business Premium Support
- IBM Security Trusteer Rapport Fraud Feeds for Retail
- IBM Security Trusteer Rapport Fraud Feeds for Retail Premium Support
- IBM Security Trusteer Rapport Phishing Protection for Business
- IBM Security Trusteer Rapport Phishing Protection for Business Premium Support
- IBM Security Trusteer Rapport Phishing Protection for Retail
- IBM Security Trusteer Rapport Phishing Protection for Retail Premium Support
- IBM Security Trusteer Rapport Mandatory Service for Business
- IBM Security Trusteer Rapport Mandatory Service for Retail

1.2 Pinpoint IBM SaaS オファリング

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

- IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile
- IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile Premium Support
- IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile
- IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile Premium Support
- IBM Security Trusteer Pinpoint Carbon Copy for Business
- IBM Security Trusteer Pinpoint Carbon Copy for Business Premium Support
- IBM Security Trusteer Pinpoint Carbon Copy for Retail
- IBM Security Trusteer Pinpoint Carbon Copy for Retail Premium Support
- IBM Security Trusteer Rapport Remediation for Retail
- IBM Security Trusteer Rapport Remediation for Retail Premium Support

1.3 Mobile IBM SaaS オファリング

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

2. 課金単位

「IBM SaaS」は、「取引文書」で規定された以下の課金単位のいずれかに従って販売されます。

a. **「対象参加者」**は、「IBM SaaS」を取得する際の課金単位です。「IBM SaaS」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、「IBM SaaS」によって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使用許諾を取得しなければならないものとします。

「IBM SaaS」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、それぞれ独立して使用許諾が必要になります。

これらのオファリングの場合、サービス提供プログラムには、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」が 1 つ含まれており、「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」ごとに、メイン・ログイン・ページおよび関連ページが付随します。「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、「IBM SaaS」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「IBM SaaS」を実行する、「IBM SaaS」にデータを提供する、「IBM SaaS」により提供されるサービスを利用する、または「IBM SaaS」にアクセスするすべての「クライアント・デバイス」に対して使用許諾を取得する必要があります。

3. 料金および課金

「IBM SaaS」に対する料金は、「取引文書」に記載されます。

3.1 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、按分ベースで算定される場合があります。

4. 遵守および監査

IBM Security Trusteer Fraud Protection オファリングへのアクセスは、「取引文書」に定められた「対象参加者」または「クライアント・デバイス」の最大数に従うものとします。お客様は、「対象参加者」または「クライアント・デバイス」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。

「対象参加者」または「クライアント・デバイス」の最大数が遵守されていることを確認するために、監査が実施される場合があります。

5. 「IBM SaaS」の「サブスクリプション期間」の更新オプション

以下のいずれか 1 つを指定することにより、「サブスクリプション期間」の終了時に「IBM SaaS」を更新するかどうかをお客様の「取引文書」に定めます。

5.1 自動更新

お客様の「取引文書」に、お客様の更新は自動更新と記載されている場合、お客様は、「取引文書」に規定されている有効期間満了日の少なくとも 90 日前までに、お客様の IBM 営業担当員または IBM ビジネス・パートナーへの書面による要求により、期間満了となる「IBM SaaS」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。IBM または IBM ビジネス・パートナーが、有効期間満了日までにかかる終了通知を受領していない場合、期間満了となる「サブスクリプション期間」は 1 年間、または「取引文書」に規定される当該更新前の「サブスクリプション期間」と同じ期間のいずれかで自動的に更新されます。

5.2 請求の継続

「取引文書」にお客様の更新は継続と記載されている場合、お客様は引き続き「IBM SaaS」にアクセスすることができ、「IBM SaaS」の利用に対して継続的に請求が行われます。「IBM SaaS」の利用を中断し、継続的な請求プロセスを停止するには、お客様は 90 日前までに、IBM または IBM ビジネス・パートナーに対し、お客様の「IBM SaaS」を解約する旨書面により通知する必要があります。お客様のアクセスの解約により、お客様には解約の効力を生じる月内の未処理のアクセス料金が請求されます。

5.3 更新が必要

「取引文書」にお客様の更新タイプは「終了」であると記載されている場合、「IBM SaaS」は「サブスクリプション期間」の満了時に終了し、お客様の「IBM SaaS」へのアクセスは削除されます。終了日以降も「IBM SaaS」の利用を継続するには、お客様の IBM 営業担当員または IBM ビジネス・パートナーに対して新規の「サブスクリプション期間」を注文し、取得する必要があります。

6. テクニカル・サポート

「IBM SaaS」の「テクニカル・サポート」が、お客様およびその「対象参加者」に対して、その「IBM SaaS」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。

「IBM SaaS」のオファリングごとに、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することができます。ただし、IBM Security Trusteer Mobile SDK オファリングおよび IBM Security Trusteer Rapport Mandatory Service オファリングは除きます。

標準サポート

- 現地時間午前 8 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「IBM 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 1 日 24 時間 週 7 日のサポート。
- お客様は、電話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「IBM 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.

7. 「IBM SaaS」オファリングの追加条件

7.1 セーフ・ハーバー原則の遵守

IBM は、欧州委員会と連携して米国商務省が開発した「米国 - EU 間のセーフ・ハーバーの枠組み」を遵守します。IBM Security Trusteer 製品は、IBM の「EU - 米国間のセーフ・ハーバー原則の証明」に含まれます。「セーフ・ハーバー」および「セーフ・ハーバー」の会社リストの詳細は、ここ (http://export.gov/safeharbor/) で確認いただけます。

7.2 お客様のサブスクリプション料金の年間引き上げ

IBM は、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、「IBM SaaS」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、初回の対象期間の開始日のアニバーサリー・デート (更新日) に発効します。この料金の調整により、お客様の「IBM SaaS」の使用許諾や「IBM SaaS」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。

7.3 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「IBM SaaS」オファリングに対してのみ、プレミアム・サポートを受ける権利を有します。

7.4 合法的使用および同意

データの収集および処理の承認

「IBM SaaS」は、お客様のセキュリティー環境およびデータの改善についてお客様を支援するように設計されています。「IBM SaaS」は、お客様が申し込んでいる「IBM SaaS」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」と対話する「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。「IBM SaaS」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、「IBM SaaS」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「ToU」の「海外への移転」の項および「データ・プライバシー」の項、ならびに本「ToU」の「共通事項」の「データ・プライバシーおよびデータ・セキュリティー」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。

IBM Security Trusteer Pinpoint オファリングの場合

収集されるデータには、ユーザーの IP アドレス、暗号化または不可逆的にハッシュ化されたユーザー ID、ドメインのクッキー (フィルタリングされない場合)、保護された「アプリケーション」およびフィッシング・サイトへの訪問、地理的位置、ならびにフィッシング・サイトに入力された資格情報が含まれる場合があります。

IBM Security Trusteer Mobile SDK オファリングおよび IBM Security Trusteer Mobile Browser オファリングの場合

収集されるデータには、ユーザーの IP アドレス、暗号化または不可逆的にハッシュ化されたユーザー ID、地理的所在地、保護された「アプリケーション」への訪問、SIM カード情報、デバイス名、およびお客様の提携関係が含まれる場合があります。

IBM Security Trusteer Rapport オファリングの場合:

収集されるデータには、ユーザーの IP アドレス、暗号化または不可逆的にハッシュ化されたユーザー ID、セキュリティー・イベント、お客様サポートのために IBM と連絡を取る目的で提供されたユーザーの名前および電子メール・アドレス、お客様の提携関係、保護されたサイトに入力された暗号化パスワード、保護された「アプリケーション」およびフィッシング・サイトへの訪問、暗号化された支払いカード番号、ならびに疑われるマルウェア、悪意による行動、または誤動作を調べるために IBM 要員がリモートで収集するファイルおよびデータが含まれる場合があります。

データ主体のインフォームド・コンセント:

この「IBM SaaS」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。「IBM SaaS」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「IBM SaaS」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。

IBM Security Trusteer Pinpoint オファリングおよび IBM Security Trusteer Mobile SDK オファリングの場合

お客様は、「IBM SaaS」の合法的な利用、および「IBM SaaS」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 Security Trusteer Rapport および IBM Security Trusteer Mobile Browser の各オファリングの場合

お客様は、「IBM SaaS」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、「IBM SaaS」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「IBM SaaS」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。

7.5 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、「個人データ」を含むコンテンツを海外で処理できることに同意するものとします。

7.6 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「IBM SaaS」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「IBM SaaS」の説明書に従って「IBM SaaS」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「IBM SaaS」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 に対して書面で通知することにより、影響を受けた「IBM SaaS」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。お客様は、以下のプロセッサーおよびサブプロセッサーに対して、「個人データ」を含むコンテンツを海外で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)	ロケーション*
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	410 Terry Ave.N Seattle, WA 98109 United States
Connectria Corp.	サブプロセッサー	10845 Olive Blvd., Suite 300 St. Louis, MO 63141 United States
IBM Israel Ltd.	サブプロセッサー	94 Derech Em-Hamoshavot 49527 Petach-Tikva Israel
IBM Corp	サブプロセッサー	1 New Orchard Rd. Armonk, NY 10504 United States

お客様は、IBM が、「IBM SaaS」の提供のために必要であると合理的に判断した場合には、通知をもって、この国一覧を変更できることに同意するものとします。

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、「個人データ」を含むコンテンツを海外で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)	ロケーション*
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・ミュンヘン
IBM Israel Ltd.	サブプロセッサー	94 Derech Em-Hamoshavot 49527 Petach-Tikva Israel

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、「個人データ」を含むコンテンツを海外で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)	ロケーション*
IBM 契約事業体	プロセッサー	「取引文書」に記載
Amazon Web Services (日本)	サブプロセッサー	日本・東京
IBM Israel Ltd.	サブプロセッサー	94 Derech Em-Hamoshavot 49527 Petach-Tikva Israel

* 上表に示されるロケーションには、「プロセッサー/サブプロセッサー」の企業オフィスの住所が含まれます。データ・センターは、示された国と同一国内に配置されます。

当事者またはその関連会社は、選択条項を除く 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。関連会社が締結した場合であっても、かかる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、本契約の条件に基づいて、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。

別紙 A

1. IBM SaaS オファリング

IBM は、スタンドアロンのサービスおよびオファリングとして、または追加のサービスおよびオファリングとして、これらのサービスを提供します。注文された特定の「IBM SaaS」オファリングは、お客様の「PoE」に記載されています。

1.1 法人向けおよび個人向けの定義

IBM Security Trusteer Fraud Protection 製品は、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。

- 「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。お客様のポリシーで、特定の中小規模ビジネスを個人向けにアクセスできる対象に分類できます。
- 「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。

1.2 IBM SaaS の基本サブスクリプション・オファリング

法人向けオファリング

- IBM Security Trusteer Rapport for Business
- IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition
- IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition
- IBM Security Trusteer Pinpoint Criminal Detection for Business
- IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile
- IBM Security Trusteer Mobile SDK for Business
- IBM Security Trusteer Mobile Browser for Business

個人向けオファリング

- IBM Security Trusteer Rapport for Retail
- IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition
- IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition
- IBM Security Trusteer Pinpoint Criminal Detection for Retail
- IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile
- IBM Security Trusteer Mobile SDK for Retail
- IBM Security Trusteer Mobile Browser for Retail

「法人向け」および「個人向け」のオファリングごとに、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 Security Trusteer Mobile SDK オファリングは除きます。

1.3 IBM Security Trusteer Rapport オファリングに対する追加の IBM SaaS サブスクリプション・オファリング

IBM Security Trusteer Rapport for Business に対して利用可能な追加オファリング

- IBM Security Trusteer Rapport Fraud Feeds for Business
- IBM Security Trusteer Rapport Phishing Protection for Business

- IBM Security Trusteer Rapport Mandatory Service for Business

IBM Security Trusteer Rapport for Retail に対して利用可能な追加オファリング

- IBM Security Trusteer Rapport Fraud Feeds for Retail
- IBM Security Trusteer Rapport Phishing Protection for Retail
- IBM Security Trusteer Rapport Mandatory Service for Retail

IBM Security Trusteer Rapport オファリングの「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 Security Trusteer Rapport Mandatory Service アドオンは除きます。

IBM Security Trusteer Rapport for Business または IBM Security 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「IBM SaaS」サブスクリプション・オファリングの前提条件です。

1.4 IBM Security Trusteer Pinpoint Malware Detection オファリングの追加の IBM SaaS サブスクリプション・オファリング

IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition または IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition で利用可能な追加オファリング

- IBM Security Trusteer Pinpoint Carbon Copy for Business

IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition または IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition で利用可能な追加オファリング

- IBM Security Trusteer Pinpoint Carbon Copy for Retail
- IBM Security Trusteer Rapport Remediation for Retail

本項に記載の追加の「IBM SaaS」オファリングごとに、追加料金でプレミアム・サポート・サブスクリプションが利用可能です。

IBM Security Trusteer Pinpoint Malware Detection for Business オファリングまたは IBM Security Trusteer Pinpoint Malware Detection for Retail オファリングのサブスクリプションは、本項に記載の関連する追加の「IBM SaaS」サブスクリプション・オファリングの前提条件です。

1.5 その他の追加の IBM SaaS サブスクリプション

上記の基本サブスクリプションの追加の「IBM SaaS」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。

1.6 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「IBM SaaS」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 Security 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 Security 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「IBM SaaS」サブスクリプション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、利用可能なスプラッシュ・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 Security Trusteer Rapport オファリング

2.1 IBM Security Trusteer Rapport for Retail および IBM Security 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 Security 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 Security 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「IBM SaaS」オファリングでは、「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「IBM SaaS」オファリングは以下で構成されます。

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

TMA は、IBM Security 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許可担当者) 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) 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、ならびに (iii) ソフトウェア使用許諾契約 (以下、「EULA」といいます。) に基づいて一般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」のみを販売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

「IBM SaaS」オファリング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許可担当者) は、お客様が申し込んでいる「IBM SaaS」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」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「IBM SaaS」オファリング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」が販売されます。お客様は、利用可能な「スプラッシュ・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、別個の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 Security 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 Security Trusteer Rapport Mandatory Service SaaS オファリング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 Security Trusteer Rapport for Business および IBM Security Trusteer Rapport for Retail の追加の IBM SaaS オファリングのオプション

IBM Security Trusteer Rapport オファリングのサブスクリプションは、以下の追加の「IBM SaaS」オファリングのサブスクリプションの前提条件です。「IBM SaaS」に「for Business」と指定がある場合は、取得された追加の「IBM SaaS」オファリングも「for Business」と指定する必要があります。「IBM SaaS」に「for Retail」と指定がある場合は、取得された追加の「IBM SaaS」オファリングも「for Retail」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。

2.2.1 IBM Security Trusteer Rapport Fraud Feeds for Business および IBM Security Trusteer Rapport Fraud Feeds for Retail

お客様 (および人数の制限なくお客様の許可担当者) は、特定「アカウント・ホルダー」のデスクトップにおけるマルウェア感染やその他のエンドポイントの脆弱性に関するイベント・データを受け取るために、TMA を使用することができます。

2.2.2 IBM Security Trusteer Rapport Phishing Protection for Business および IBM Security Trusteer Rapport Phishing Protection for Retail

お客様 (および人数の制限なくお客様の許可担当者) は、フィッシングが疑われるサイトまたは詐欺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、「IBM SaaS」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。

2.2.3 IBM Security Trusteer Rapport Mandatory Service for Business および IBM Security Trusteer Rapport Mandatory Service for Retail

お客様は、お客様が申し込んでいる「IBM SaaS」オファリング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 Security Trusteer Rapport Premium Support for Business は、IBM Security Rapport Mandatory Service for Business の前提条件です。

IBM Security 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 Security 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「IBM SaaS」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」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。

3. IBM Security Trusteer Pinpoint オファリング

IBM Security 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「IBM SaaS」オファリングの範囲および詐欺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「IBM SaaS」オファリングは以下で構成されます。

a. TMA

TMA は、IBM Security 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許可担当者) 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. Web スクリプトおよび API

「IBM SaaS」にアクセスする、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 Security Trusteer Pinpoint Malware Detection および IBM Security Trusteer Pinpoint Criminal Detection

IBM Security Trusteer Pinpoint Malware Detection オファリングのマルウェア検出、または IBM Security Trusteer Pinpoint Criminal Detection オファリングの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 Security Trusteer Pinpoint Malware Detection オファリングおよび IBM Security Trusteer Pinpoint Criminal Detection オファリングについては、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 Security Trusteer Pinpoint 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)。

3.1.1 IBM Security Trusteer Pinpoint Criminal Detection for Business および IBM Security 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盗難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 Security Trusteer Pinpoint Criminal Detection 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 (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) 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許可担当者) は、お客様が申し込んでいる「IBM SaaS」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」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。

3.1.2 IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile および IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile

IBM Security Trusteer Pinpoint Criminal Detection for Mobile (PPCD Mobile) オファリングは、別の保護層を提供するように設計されています。また、犯罪によるアカウントへのアクセスを特定することにより、およびお客様に推奨を行うことにより、アカウント乗っ取り活動および詐欺行為から保護することを目的としています。本「IBM SaaS」オファリングでは、PPCD Mobile API を使用して、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) ならびに「対象参加者」のモバイル・デバイスの両方から発信される情報を収集します。IBM Security Trusteer PPCD Mobile オファリングは、「対象参加者」のモバイル・デバイスに関連する複雑な情報を別のデータ・ソース (本「ToU」に記載された IBM Security Trusteer のその他の「IBM SaaS」オファリングを通じて統合される、マルウェア感染およびフィッシングに関するリアルタイムのインシデントなど) と関連付けられるように設計されています。

お客様は、IBM Security Trusteer のクラウド・ホスティング環境で、IBM Security Trusteer PPCD Mobile オファリングにアクセスしてそれらを使用し、「対象参加者」のモバイル・デバイスから、お客様が申し込んでいる「IBM SaaS」オファリング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」とこれらのモバイル・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リスク評価データを受け取ることができます。これら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携帯電話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。

3.1.3 IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition および IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition および IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition および IBM Security 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 Security Trusteer Pinpoint Malware Detection オファリングは、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詐欺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許可担当者) 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 1000 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「IBM SaaS」オファリングのコア機能を提供する、即導入可能なソリューションです。

3.2 IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition および IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition および IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition および IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition に対する追加の IBM SaaS オファリングのオプション

IBM Security Trusteer Rapport Remediation for Retail オファリングについては、IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition または IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition が前提条件となります。

IBM Security Trusteer Pinpoint Carbon Copy for Retail については、IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition または IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition が前提条件となります。IBM Security Trusteer Pinpoint Carbon Copy for Business については、IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition または IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition が前提条件となります。

3.2.1 IBM Security Trusteer Pinpoint Carbon Copy for Business および IBM Security Trusteer Pinpoint Carbon Copy for Retail

IBM Security 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「IBM SaaS」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時点を特定するのに役立ちます。

3.2.2 IBM Security Trusteer Rapport Remediation for Retail

IBM Security Trusteer Rapport Remediation for Retail は、IBM Security 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、お客様の「個人向けアプリケーション」に限定的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、修復、ブロック、および削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 Security Trusteer Pinpoint Malware Detection 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、修正するためのツールとしてのみ、本「IBM SaaS」オファリングを利用することができます。IBM Security Trusteer Rapport Remediation 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。明確にするため記すと、本「IBM SaaS」オファリングには、お客様の一般的な「対象参加者」全般に該当しない第三者に対して、その他の方法で、Trusteer Splash の使用権および「アカウント・ホルダーのクライアント・ソフトウェア」の販売を促進する権利 (またはそのいずれか) は含まれていません。

4. IBM Security Trusteer Mobile オファリング

4.1 IBM Security Trusteer Mobile Browser for Business および IBM Security Trusteer Mobile Browser for Retail

IBM Security 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「IBM SaaS」オファリングの範囲、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「IBM SaaS」オファリングの場合、モバイル・デバイスには携帯電話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 (および人数の制限なくお客様の許可担当者) 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「IBM SaaS」オファリング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」のみを販売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許可担当者) は、お客様が申し込んでいる「IBM SaaS」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」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「IBM SaaS」オファリング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」が販売されます。お客様は、利用可能なスプラッシュ・テンプレート (以下、「スプラッシュ・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、別個の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 Security 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。

4.2 IBM Security Trusteer Mobile SDK for Business および IBM Security Trusteer Mobile SDK for Retail

IBM Security Trusteer Mobile SDK オファリングは、お客様が申し込んでいる「IBM SaaS」オファリングの範囲、サブスクリプション、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 Security Trusteer Mobile SDK オファリングには、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 Security 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「IBM SaaS」オファリング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 Security 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 Security 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 Security 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許可担当者) 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携帯電話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 Security 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「ToU」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」を販売して配布すること。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」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「IBM SaaS」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 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。

お客様は、お客様による IBM Security Trusteer Mobile SDK の使用が本「ToU」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。

5. IBM SaaS Fraud Protection オファリングの導入

お客様の基本的なサブスクリプションには、必要なセットアップおよび初回の導入作業 (初回のワンタイム・スタートアップ、構成、「スプラッシュ・テンプレート」、試験、および研修など) が含まれています。

追加のサービスは、追加料金にて、別個の合意書に基づいて契約することができます。

別紙 B

IBM は、「IBM SaaS」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、お客様の「取引文書」で指定される場合には、この SLA が適用されます。

開始時またはお客様の「サブスクリプション期間」の更新時における最新版の本 SLA の条件が、適用されます。お客様は、SLA が、お客様に対し何ら保証するものでないことを理解します。

1. 定義

a. **「権限を有する担当者」**- お客様が IBM に対して指定している、本 SLA に基づき「請求」を提出することが認められた個人をいいます。

b. **「可用性クレジット」**- IBM が検証した「請求」に対して提供する救済措置をいいます。「可用性クレジット」は、返金または「IBM SaaS」のサブスクリプション料金の将来の請求額から割り引く形で適用されます。

c. **「請求」**- 本 SLA に基づいて、お客様の「権限を有する担当者」が IBM に対して提出する、「契約月」中に「サービス・レベル」が満たされていない旨の主張をいいます。

d. **「契約月」**- その月の初日の午前 12 時 (グリニッジ標準時) から当該月の末日の午後 11 時 59 分 (グリニッジ標準時) までを基準とする「IBM SaaS」期間における各 1 か月をいいます。

e. **「お客様」**- IBM に対して「IBM SaaS」を直接申し込み、IBM との「IBM SaaS」に関する契約に基づく重大な義務 (支払義務を含みます。) に違反していない法人または団体をいいます。

f. **「ダウン時間」**-「サービス」のための実稼働システム処理が停止し、適切な許諾を得ているすべてのお客様のユーザーが、あらゆる「サービス」を利用できなくなる期間をいいます。「ダウン時間」には、「サービス」が以下のいずれかに起因して利用できなくなった場合の期間は含まれません。

- 計画されたシステムのダウン時間。
- 不可抗力。
- お客様または第三者のアプリケーション、機器またはデータの不具合。
- お客様または第三者 (お客様のパスワードまたは機器を使用して「IBM SaaS」へアクセスするあらゆる利用者を含みます。) の作為または不作為。
- 「IBM SaaS」にアクセスするための所要のシステム構成およびサポートされているプラットフォームを満たさないこと。
- IBM が、お客様またはお客様に代わる第三者が提供する設計、仕様、または指示に従った場合。

g. **「事象」**-「サービス・レベル」が満たされない原因となる状況または一連の状況をいいます。

h. **「不可抗力」**- 天災、テロリズム、労働争議、火災、洪水、地震、暴動、戦争、政府による法令、命令もしくは制限、ウィルス、サービス妨害攻撃およびその他の悪意の行為、ユーティリティーおよびネットワーク接続の不具合、または IBM が合理的に制御できないサービスが利用できなくなるその他の原因をいいます。

i. **「計画されたシステムのダウン時間」**- 保守作業のための定期的な「IBM SaaS」の停止をいいます。

j. **「サービス・レベル」**- IBM が本 SLA に規定するサービスのレベルを評価するための、以下に定める基準をいいます。

2. 可用性クレジット

a. お客様が、「請求」するには、IBM の重要度 1 のサポート問題の報告手順に従って、各「事象」に対するサポート・チケットを、該当する「IBM SaaS」の IBM お客様サポート・ヘルプ・デスクに対して、記録しなければなりません。お客様は、「事象」に関するすべての必要な詳細情報を提出し、「事象」の分析および解明につき、重要度 1 のサポート・チケットが要求する範囲で IBM を合理的に支援しなければなりません。かかるチケットは、「事象」がお客様の「IBM SaaS」の利用に影響を与えていることをお客様が最初に認識してから 24 時間以内に記録しなければなりません。

b. お客様の「権限を有する担当者」は、お客様の「可用性クレジット」の「請求」を、「請求」の対象となる「契約月」の末日から 3 営業日以内に提出しなければなりません。

c. お客様の「権限を有する担当者」は、「請求」に関するあらゆる合理的な詳細 (関連するすべての「事象」および満たされていないとして請求される「サービス・レベル」についての詳細な説明を含みますがこれらに限られません。) を、IBM に提供しなければなりません。

d. IBM は、以下の表に示した対応する「サービス・レベル」に適用可能な、各「契約月」中における「ダウン時間」の合計時間を内部で測定します。「可用性クレジット」は、「ダウン時間」が最初に影響を与えたことがお客様により報告された時点から測定されるダウン時間に基づいて決定されます。お客様が、「アプリケーション・ダウン時間」の「事象」と「インバウンド・データ処理ダウン時間」の「事象」が同時に発生したと報告した場合、IBM は「ダウン時間」の重複する期間を、2 つの別のダウン時間としてではなく 単一のダウン時間として扱います。IBM は、有効な「請求」それぞれに対し、下表に示した各「契約月」において達成した「サービス・レベル」に基づき、適用可能な「可用性クレジット」の最高額を適用します。同「契約月」中における同「事象」に対する「可用性クレジット」は、重複して適用されません。

e. 「一括サービス」(個別の「IBM SaaS」を組み合わせてパッケージとし、単一料金で販売しているもの) に対する「可用性クレジット」は、「一括サービス」に対する合計の単一月額料金に基づいて計算されるものとし、各個別「IBM SaaS」に対する月額サブスクリプション料金には基づかないものとします。お客様は、すべての「契約月」において、一括で、1 つの個別の「IBM SaaS」に関する「請求」のみ提出することができます。また、IBM は、すべての「契約月」において、一括で、2 つ以上の「IBM SaaS」に対する「可用性クレジット」に関する責任を負いません。

f. お客様が、認定された IBM ビジネス・パートナーからの再販売取引によって「IBM SaaS」を購入した場合で、IBM が「IBM SaaS」および SLA のコミットメントを履行する一義的な責任を負う場合、「可用性クレジット」は、「請求」の対象となる「契約月」において有効な「IBM SaaS」に対するその当時の「レベル別推奨数量割引料金」(以下、「RSVP」といいます。) に基づいて計算され、それを、50% 割引した額となります。

g. すべての「契約月」に支払われた「可用性クレジット」の合計額は、いかなる状況においても、お客様が「IBM SaaS」に対して IBM に支払った年額料金の 1/12 の 10% を超えないものとします。

h. IBM は、IBM の記録から入手し得る情報に基づいて、「請求」の検証を合理的に判断します。お客様の記録におけるデータと IBM の記録の間で相違がある場合には、IBM の記録が優先するものとします。

i. 本 SLA に基づいてお客様に提供される「可用性クレジット」は、「請求」に関するお客様の唯一かつ排他的な救済措置です。

3. サービス・レベル

「契約月」における「IBM SaaS」の可用性

達成したサービス・レベル (「契約月」中)	**「可用性クレジット」 (「請求」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パーセント)**
<99.5%	2%
<98.0%	5%
<96.0%	10%

「達成したサービス・レベル」は、以下のとおり算出されます。(a)「契約月」における分単位の総時間数から、(b)「契約月」における「ダウン時間」の分単位の総時間数を差し引き、それを (c)「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。

例:「契約月」における総「ダウン時間」250 分

30 日の「契約月」における合計 43,200 分 －「ダウン時間」250 分＝ 42,950 分 合計 43,200 分	＝「契約月」における 99.4% の「達成したサービス・レベル」につき 2% の「可用性クレジット」

3.1 除外事項

本 SLA は、IBM のお客様に限り、適用されます。本 SLA は、以下の場合には適用されません。

- ベータ版および評価版の「サービス」。
- 非実稼働環境 (テスト、災害復旧、品質保証、または開発用環境を含みますが、これらに限られません)。
- 「IBM SaaS」における IBM のお客様のユーザー、ゲスト、参加者、および許可された招待者による「請求」。
- お客様が、本「ToU」に基づく重要な義務に違反した場合。これには支払義務の違反が含まれますが、これに限られません。