IBM クラウド・サービス記述書

IBM Security AppScan Mobile Analyzer

お客様の注文に関する「サービス記述書」は、以下のとおりです。

1. クラウド・サービス

「クラウド・サービス」オファリングについては、以下に記載されており、一部の使用許諾されたオファリングの「注文関連文書」で指定されています。「注文関連文書」は、提供されている「見積書」および「クラウド・サービス」の開始日および期間を確認する「証書 (PoE)」で構成されます。請求は、「クラウド・サービス」のプロビジョニング後に開始されます。

1.1 IBM Security AppScan Mobile Analyzer

本サービスは、Android モバイル・アプリケーションのコード・レベルでセキュリティーの問題を特定します。また、開発者はアプリケーションのソース・コードを供する必要なく、スキャンを実行してセキュリティーの脆弱性を見つけ出すことができます。スキャンが終わると、本サービスはセキュリティー・レポートを生成します。このレポートには、検出した脆弱性、かかる脆弱性により引き起こされる可能性のあるモバイル・アプリケーションに対するセキュリティー・リスクが、それらの修正方法に対する推奨とともに記載されます。

2. セキュリティーの内容

2.1 セキュリティー・ポリシー

IBM は、情報セキュリティー・チームを保有し、また、プライバシーおよびセキュリティーに関するポリシーを IBM の従業員に伝え、これを保持します。IBM は、IBM データ・センターをサポートする要員に対し、プライバシーおよびセキュリティーに関する研修の受講を要求します。IBM セキュリティー・ポリシーおよび基準については年 1 回、審査し、再評価します。IBM のセキュリティーに関する事故は、包括的な事故対応手順に従って処理されます。

2.2 アクセス制御

クライアント・データに対するアクセスは、必要に応じて、職務分離の原則に従って、権限のある IBM サポート担当員およびサービス実施担当者によってのみ許可されます。IBM スタッフは、中間「ゲートウェイ」管理ホストに二要素認証を使用します。クライアント・データにアクセスする際のすべてのチャネル接続は暗号化されます。

2.3 サービスの完全性および可用性

オペレーティング・システムおよびアプリケーション・ソフトウェアの変更には、IBM の変更管理プロセスが適用されます。また、ファイアウォール規則の変更についても変更管理プロセスが適用され、導入前に IBM セキュリティー・スタッフが審査します。IBM はデータ・センターを 1 日 24 時間週 7 日体制で監視します。潜在的なシステム・セキュリティー危険度の検出および解決を支援するために、内部および外部の脆弱性スキャニングを権限のある管理者および第三者ベンダーが定期的に実施します。マルウェア検出 (アンチウィルス、侵入検知、脆弱性スキャニングおよび侵入防止) システムは、すべての IBM データ・センターで使用されています。IBM のデータ・センター・サービスは、公共ネットワーク上のデータ伝送についてさまざまな情報伝送プロトコルをサポートします。これには、HTTP/SFTP/FTP/S/MIME、サイト間 VPN などが含まれます。オフサイトで保管されるバックアップ・データは、転送前に暗号化されます。

2.4 アクティビティーの記録

IBM は、アクティビティーを記録する機能があり、そのように構成された、システム、アプリケーション、データ・リポジトリー、ミドルウェア、およびネットワーク・インフラ・デバイスに関して、アクティビティーのログを保持します。改ざんの可能性を最小限に抑え、集中型分析、アラートおよびレポートを可能にするために、アクティビティーは中央ログ・リポジトリーにリアルタイムで記録されます。改ざんを防ぐために、データを署名付きにします。異常な行動を検出するために、ログはリアルタイ

ムで、また、定期的な分析レポートによって分析されます。運用スタッフは異常に関するアラートを受け、必要に応じて 1 日 24 時間週 7 日、オンコールのセキュリティー・スペシャリストに連絡を取ります。

2.5 物理的セキュリティー

IBM は、IBM データ・センターに対する許可されていない物理的アクセスを制限するように設計された物理的セキュリティー基準を保持します。データ・センターには制限されたアクセス・ポイントのみが存在し、アクセス・ポイントは二要素認証で制御され、監視カメラによって監視されています。アクセスは、アクセスを承認された権限のあるスタッフのみに許可されます。運用スタッフは承認について確認し、必要なアクセスを提供するアクセス・バッジを発行します。かかるバッジを交付された従業員は、他のアクセス・バッジを返却しなければならず、そのアクティビティーの期間中はデータ・センター・アクセス・バッジのみを所持することができます。バッジの使用については、記録されます。IBM 以外の訪問者は、施設に入場する際に登録され、施設内にいる間は付添人が同行します。搬入・搬出場所、および許可されていない個人が施設に入場できるその他の場所については管理され、隔離されます。

2.6 遵守

IBM はプライバシーの実践が米国商務省の「セーフ・ハーバー原則」(通知、選択、転送、アクセスおよび正確性、セキュリティー、ならびに監督/実施) に一致することを年 1 回証明します。IBM は、業界基準の SSAE 16 監査 (または同等の監査) を、実稼働データ・センターで年 1 回実施します。IBM は、IBM の事業要件の遵守に関してセキュリティーおよびプライバシー関連のアクティビティーを審査します。情報セキュリティー・ポリシーの遵守を確認するために、IBM は評価および監査を定期的に実施します。IBM の従業員およびベンダーの従業員は、全従業員向けのセキュリティーおよび意識向上研修を年 1 回受講します。倫理的な企業行動、機密保持および IBM のセキュリティー義務を果たすために、従業員は年 1 回、自身の業務目標および責任について再認識します。

3. エンタイトルメントおよび課金情報

3.1 課金単位

「クラウド・サービス」は、「注文関連文書」で規定された以下の課金単位に従って利用することができます。

- 「アプリケーション・インスタンス」は、「IBM SaaS」を取得する際の課金単位です。「IBM SaaS」に接続された「アプリケーション」の「インスタンス」ごとに、「アプリケーション・インスタンス」の使用許諾が必要です。「アプリケーション」に複数のコンポーネントが含まれており、各コンポーネントが、別々の目的を果たす、別々のユーザー・ベースである、別々の接続を持っているなどといった場合には、かかる各コンポーネントは、個別の「アプリケーション」と見なされます。さらに、「アプリケーション」のテスト、開発、ステージング、および実稼働の各環境は、それぞれが「アプリケーション」の個別のインスタンスと見なされ、それぞれについて使用許諾を取得する必要があります。1 つの環境に含まれた「アプリケーション」の複数のインスタンスは、それぞれが「アプリケーション」の個別のインスタンスと見なされ、それぞれについて使用許諾を取得する必要があります。お客様の「証書 (PoE)」または「取引文書」に定める課金期間中に「IBM SaaS」に接続された「アプリケーション・インスタンス」の数をカバーするのに十分な使用許諾を取得する必要があります。

3.2 料金および課金

「クラウド・サービス」に関する支払金額は、「注文関連文書」に記載されます。

3.3 従量制課金

従量制課金オプションは、お客様がサービスを使用した翌月に「取引文書」に記載された料金で請求されます。

4. テクニカル・サポート

「サブスクリプション期間」中、「クラウド・サービス」に対する「テクニカル・サポート」が提供されます。

「運用に関するサポート時間」は、以下のとおりです。

利用可能時間、オンライン問題報告システム、およびその他のテクニカル・サポートに関する伝達手段や伝達プロセスに関する情報は、IBM Software as a Service (SaaS) Support Handbook に記載されています。

営業時間外サポート

営業時間外サポート (上記の通常営業時間以外) は、重要度 1 の問題についてのみ、営業日、週末および休日に利用可能です。重要度 1 の問題の場合、お客様には、1 日 24 時間 週 7 日、問題の診断を支援することが求められます。かかる支援ができない場合には、問題は重要度 2 にダウングレードされます。

4.1 フォーラム・サポート

「クラウド・サービス」のすべてのお客様には、IBM サポート担当員および開発者が定期的にモニターするフォーラム・サポートが提供されます。

a. 質問をする:

https://developer.ibm.com/answers/questions/ask/?topics=appscan-mobile-analyzer

b. 現在の投稿を表示する:

https://developer.ibm.com/answers/topics/appscan-mobile-analyzer/

4.2 標準サポート

お客様に従量制課金が課される期間中、標準サポートを利用することができます。「クラウド・サービス」内から、お客様はサポート・チケットを送信したり、支援用チャット・セッションをオープンしたりできます。サポートの手順について詳しくは、IBM サポート Web ポータル (https://support.ibmcloud.com) または「IBM SaaS ソフトウェア・サポート・ハンドブック」 (http://www.ibm.com/software/support/acceleratedvalue/SaaS_Handbook_V18.pdf) をご覧ください。

重要度	重要度の定義	目標応答時間	対象応答時間
1	**重大な事業影響/サービス・ダウン** 事業上の重大な機能を実行することができない、または重要なインターフェースが機能しない状態。これは通常実稼働環境に適用され、サービスにアクセスできないことによって業務上重大な影響が生じることを示します。この状況は、即時に解決する必要があります。	1 時間以内	1 日 24 時間週 7 日
2	**著しい事業影響** サービス事業機能またはサービスの機能が著しい使用制限を受けているか、または、お客様が事業の最終期限に間に合わない危険にさらされている状態。	2 営業時間以内	月曜から金曜の営業時間
3	**軽度の事業影響** サービスまたは機能を使用でき、業務上、重大な影響がないことを示す。	4 営業時間以内	月曜から金曜の営業時間
4	**最小の事業影響** 問い合わせまたは非技術的な要求。	1 営業日以内	月曜から金曜の営業時間

5. セーフ・ハーバー原則の遵守

IBM は、本「クラウド・サービス」について「米国 - EU 間のセーフ・ハーバーの枠組み」および「米国 - スイス間のセーフ・ハーバーの枠組み」の遵守を決定していません。

6. 追加情報

「クラウド・サービス」は、モバイル・アプリケーションおよびモバイル Web サービスのセキュリティーおよび適合性に関する潜在的な問題を特定できるように設計されています。「クラウド・サービス」は脆弱性およびコンプライアンスに関するすべてのリスクをテストするわけではなく、また、セキュリティー攻撃に対する障壁の役目も果たしません。セキュリティーの脅威、規制および標準は変化し続けているため、「サービス」はかかる変更のすべてを反映できません。お客様のモバイル・アプリケーション、システムおよび従業員のセキュリティーとコンプライアンス、救済措置についても、お客様が一切の責任を負います。「サービス」によって提供される情報を使用するかどうかは、お客様の判断に一任されます。

6.1 Derived Benefit Locations

該当する場合、税金は、お客様が「クラウド・サービス」の恩恵を受けているとお客様がみなす場所に基づきます。IBM は、お客様が IBM に追加情報を提供する場合を除き、「クラウド・サービス」の注文時に主に恩恵を受ける場所として記載した事業所住所に基づいて税金を適用します。お客様は、当該情報を最新に保ち、変更があった場合には IBM に通知する責任を負うものとします。

6.2 Cookie

お客様は、IBM が「クラウド・サービス」の通常の運用およびサポートの一部として、トラッキングおよびその他の技術により、「クラウド・サービス」の使用に関連してお客様 (お客様の従業員および従契約者) から個人情報を収集できることを了解し、これに同意するものとします。IBM は、ユーザー・エクスペリエンスの向上およびお客様との対話の調整またはそのいずれかを目的として、「クラウド・サービス」の有効性について使用統計および情報を集めるためにこうした情報収集を行います。お客様は、IBM およびその従契約者が、営業活動を行う地域で、適用法に従い、IBM、その他の IBM グループ会社およびそれぞれの従契約者の範囲内で、収集した個人情報を以上の目的のために処理できるように、お客様が同意を取得する意向であること、または取得済みであることを確認します。IBM は、収集した個人情報へのアクセス、更新、修正または削除について、お客様の従業員および従契約者からの要求に従います。