

IBM QRadar on Cloud

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

1.1 IBM QRadar on Cloud 100 EPS

IBM QRadar on Cloud オファリングは、IBM Security QRadar SIEM 製品に基づいて IBM クラウドから高度なセキュリティー・インテリジェンス・ソリューションを提供します。このオファリングにより、お客様は、オンプレミス環境およびクラウド環境から生成されるイベントの収集、相関関連付け、および保管ができるほか、オンプレミス上に展開された QRadar SIEM 製品で行われるとおりに、セキュリティーおよび脅威管理を実行できます。当該オファリングの一部として、IBM は 1 日 24 時間 週 7 日体制でインフラストラクチャー・モニタリングを提供し、最新のソフトウェア・レベルのパッチまたは重要なパッチが提供された場合にはそれらを適用します。

本「クラウド・サービス」には、有効で検索可能な 90 日間のストレージが含まれます。

1.2 オプションの機能またはサービス

1.2.1 IBM QRadar on Cloud 1K EPS Temporary Upgrade

ログ・イベントの収集と処理のための追加の 1000 EPS キャパシティーを提供するサービス・アップグレード (ただし、一時的な月数に限られます。)。お客様はこのアップグレードについて、当該オファリングがサポートできる最大 EPS レベルを上限に、複数のユニットを購入できます。この部分は、当該年の間の「スパイク (急増)」時のカバレッジを必要とするお客様が、一時的にキャパシティーのアップグレードによりこれらの要件を満たせるようにすることを目的としています。当該期間の終了時点で、これらの一時的なキャパシティーの増分はお客様の環境から削除されます。

1.2.2 IBM QRadar on Cloud Data Capacity 100 EPS

データ容量アップグレードにより、追加的ストレージが追加され、分析期間が拡張されます。容量アップグレードにより、お客様は、購入した 100 EPS アップグレードごとに最大で 1 年間の保管データを入力できます。

1.2.3 IBM QRadar on Cloud Flows Add-On

IBM QRadar SIEM およびフロー・プロセッサと統合して、「レイヤー 3」ネットワークの可視性およびフロー分析を提供し、お客様がお客様のネットワーク全体のアクティビティーを検知、検出およびそれに対応できるようにします。

1.2.4 IBM QRadar on Cloud Vulnerability Management Add-On

ネットワーク・デバイスおよびアプリケーションのセキュリティーの脆弱性を事前に検知および発見し、コンテキストを追加して、修復アクティビティーおよび緩和アクティビティーの優先順位をサポートします。

1.2.5 IBM QRadar on Cloud Log Archival

お客様は、サブスクライブした期間中、「クラウド・サービス」からのイベント・データを保存できます。IBM はお客様と協力して、保存のためにオブジェクト・ストレージに指定されたイベントを書き込みます。お客様の要求を受けて、IBM はかかる要求から 3 営業日以内に、最大 30 日分の保存イベント・データを、「クラウド・サービス」のおお客様のインスタンスに再マウントします。かかるデータは、保存オブジェクト・ストレージに戻される前に、48 時間利用できます。お客様は、3 か月ごとに最大 2 回要求できます。容量アップグレードにより、お客様は、購入した 100 EPS アップグレードごとに最大で 1 年間の保管データを入力できます。

1.2.6 IBM QRadar on Cloud Optimization Service

このリモートで提供されるサブスクリプション・サービスについて、IBM はお客様とレビュー会議を実施して、お客様の「クラウド・サービス」インスタンスに関する現在の正常性を評価し、QRadar on Cloud ヘルス・ステータス・レポート経由でお客様に結果を提供します。このレポートでは、改善する領域がある場合には、それを指定します。

さらに、IBM はお客様の要求に応じて、1 年間に最大 8 日間、以下のコンサルティング・サービスをお客様に提供します。

- 「クラウド・サービス」に新たなログ・ソースを追加する際の支援。
- 追加の検索、レポートおよびダッシュボードの構成。
- 既存の QRadar 導入に対する追加チューニングの実施。
- 関連する QRadar 対象に関するナレッジ・トランスファーの実行。

1.3 セットアップ・サービス

以下のセットアップ・サービスはリモートで提供されるもので、別途注文可能です。注文された各サービスは、すべての時間 (該当する場合) が使用されたかどうかに関係なく、別途記載のない限り、購入から 90 日後に失効します。サービスには、キックオフ電話会議のスケジュールを設定する指定された IBM Engagement Manager が含まれます。

1.3.1 IBM QRadar on Cloud Deployment Service

このサービスでは、40 時間のプロフェッショナル・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。

IBM は、お客様のレポート要件を定義するために最大 16 時間の SIEM アーキテクチャー・レビューを実施し、ソリューション・アーキテクチャー・レポートで所見をお客様に提供します。このレポートは、お客様の要件の定義と取り込みに役立つものになります。

このレポートには以下が含まれます。

- お客様の法令遵守、監査、セキュリティ・インテリジェンスに関する要件を満たすのに役立つ、お客様定義のレポート要件。
- IBM が実装を支援できるセキュリティ・インテリジェンス要件、ユース・ケース、およびアプリ (最大 10 件のユース・ケースと最大 2 個のアプリ)。
- ユース・ケースをサポートする必要がある、お客様のログおよびフロー・ソースに関する大まかな情報。
- ネットワーク・インフラストラクチャーに関する懸念事項 (ファイアウォールおよびポートなど)。

このソリューション・アーキテクチャー・レポートに基づいて、IBM は残余時間の許す限り、以下のタスクを実行します。

- 最大 10 のログ・ソース・タイプの最大 3 つのインスタンスに対してイベントのコレクションを構成します。このアクティビティには、必要に応じてさらにログ・ソースを追加できるよう、お客様の関連担当者へのナレッジ・トランスファーが含まれます。標準の QRadar Device Support Modules (DSMs) でサポートされるログ・ソースのみが、本サービスの一部として含まれます。
- 初期チューニング。これには、a) すぐに使用できるルール of アクティブ化、節約された検索、時系列 (累積型) のグラフとレポート、b) ノイズの特定と削除、および c) NFS、CIFS、または iSCSI を経由したオフライン・ストレージの構成が含まれます。
- 10 件のユース・ケースと 2 個のアプリを、ソリューション・アーキテクチャー文書に記録された IBM QRadar App Exchange から実装します。

1.3.2 IBM QRadar on Cloud Custom Parser Service

このサービスでは、お客様の非標準のログ・ソース・タイプのうち、「クラウド・サービス」に送信されるものをサポートするために単一のカスタム・パーサー、カスタム uDSM を開発します。このサービスには、以下のタスクが含まれます。

- 1つの非標準のログ・ソース・タイプ用にカスタム・パーサーを作成します(リモートで実行される作業)。
- uDSM を作成、構成、およびマッピングします。
- カスタム uDSM を導入してテストします。
- 当該ログ・ソースに対する最大 25 のメッセージ・タイプを解析します。

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、発生する処理活動、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書に関する、「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、「クラウド・サービス」のお客様による使用に適用される「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の慣行にかかわらず、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 のみの裁量により、「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) 既存のコミットメント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、または iii) 追加コミットメント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」のいかなる変更も「クラウド・サービス」のデータ保護を著しく低下させるものではありません。

適用される「データ・シート」へのリンク:

<https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=FB0F42F0750011E6865BC3F213DB63F7>

お客様は、「クラウド・サービス」の利用可能なデータ保護機能を注文、有効化、または使用するために必要な対策を講じる責任を負うものとします。お客様がかかる対策を講じることを怠った場合(「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。)には、お客様は「クラウド・サービス」の使用に対して責任を負います。

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」に適用可能な「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関する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。

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」が利用できず、業務に重大な影響が及んだことを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 (申告の対象である「契約月」における 「月額サブスクリプション料金」* の割合)
99.9% 未満	2%
99% 未満	5%
95% 未満	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。

「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「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。

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、電子メール、オンライン・フォーラム、およびオンライン問題報告システムを介して提供されます。IBM の IBM Software as a service support guide (https://www-01.ibm.com/software/support/saas_support_guide.html) には、テクニカル・サポートの連絡先情報ならびにその他情報およびプロセスが規定されています。テクニカル・サポートは「クラウド・サービス」と共に提供されるものであり、別個のオフリングとして提供されるものではありません。

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。
- 「1 秒あたりのイベント (EPS)」は、「クラウド・サービス」を取得する際の課金単位です。「イベント」とは、「クラウド・サービス」が処理する、または「クラウド・サービス」の利用に関連する、特定のイベントが 1 回発生することをいいます。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」が収集または処理する 1 秒あたりの「イベント」の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。
- 「1 分あたりの 1 万フロー」は、「クラウド・サービス」を取得する際の課金単位です。「フロー」とは、2 つのホスト間の通信記録です。同じソース IP、宛先 IP、ソース・ポート、宛先ポート、およびプロトコルを含むパケットはすべて結合されて、1 つの「フロー」記録になります。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」が管理または処理する、

1 分間の最大「フロー」数 (1 万単位で切り上げ) 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。

- 「256 資産」は、「クラウド・サービス」を取得する際の課金単位です。「資産」とは、管理対象となる、あらゆる有形リソースまたは項目をいいます。これには、実稼働設備、施設、輸送機関、IT ハードウェアおよび IT ソフトウェアが含まれます。「クラウド・サービス」で固有 ID を保持するリソースまたは項目は、別個の「資産」となります。お客様の「証書 (PoE)」または「取引文書」に定める課金期間中に「クラウド・サービス」がアクセスまたは管理する「資産」(256 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。各「256 資産」のエンタイトルメントは「256 資産」を表します。

5.2 セットアップ料金

1 回限りのセットアップ料金は、発注された各セットアップ・サービスに対して「取引文書」に記載された料金で請求されます。

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、後払いの対象となる超過分や料金の使用タイプは除きます。

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」が自動的に更新されるか、継続利用ベースで続行されるか、期間満了時に終了するかが記載されます。

自動更新の場合には、お客様が期間満了日の少なくとも 90 日前までに書面により更新しないことを通知する場合を除き、「クラウド・サービス」は、「PoE」に定める期間につき自動更新されます。更新には、見積書に記載されたとおりに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、現在の更新終了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、「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 イネープリング・ソフトウェア

本「クラウド・サービス」には、「クラウド・サービス」期間にわたって、「クラウド・サービス」のお客様による使用に関連してのみ使用することのできるイネープリング・ソフトウェアが含まれます。イネープリング・ソフトウェアに別途付帯するご使用条件がある場合、本項で制限されるとおり、かかるご使用条件の期間も適用されます。矛盾が生じた場合、本「サービス記述書」の条件が、これらの付帯するご使用条件すべてに優先するものとします。イネープリング・ソフトウェアは現状のまま提供されます。お客様は「イネープリング・ソフトウェア」のコピーを最大 10 件インストールして使用することのみ可能です。

7.3 セキュアなデータ

IBM は、サイバー脅威インテリジェンスの文脈で使用する目的で、お客様の「コンテンツ」から悪意のあるアクティビティの可能性を示す指標を収集する場合があります。具体的には、URL、IP アドレス、ドメイン、およびファイル・ハッシュです。さらに IBM は、こうした指標により、お客様のサイバー脅威のリスクが高まっていることが示唆されている場合には、お客様に通知する場合があります。