IBM QRadar on Cloud

本「サービス記述書」は「クラウド・サービス」について規定するものです。適用できる注文関連文書には、お客様の発注に関する価格設定および追加的な詳細情報が記載されています。

1. クラウド・サービス

1.1 IBM QRadar on Cloud

お客様は、利用可能な以下のオファリングから選択することができます。

1.1.1 IBM 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・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)」時のカバレージを必要とするお客様が、一時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 Storage 100 EPS

データ・ストレージ・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、100 EPS アップグレードの購入ごとに最大で 1 年間の保管データを入手できます。

1.2.3 IBM QRadar on Cloud Flows Add-On

IBM QRadar SIEM およびフロー・プロセッサーと統合して、「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手できます。

1.3 Acceleration Services

1.3.1 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 Health Status 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 導入に対する追加調整の実施。
- 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。

1.3.2 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。

1.3.3 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、セキュリティー・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ー・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のある、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ーには、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。
- 初期調整。これには、a) すぐに使用できるルールのアクティブ化、節約された検索、時系列 (累積型) のグラフとレポート、b) 音源の特定と削除、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。

1.3.4 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 /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。
- カスタムの 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. データ処理およびデータ保護に関するデータ・シート

IBM のデータ処理補足契約書 (http://ibm.com/dpa に公開。「DPA」) のほか、下記リンクの「データ処理およびデータ保護に関するデータ・シート」 (データ・シートまたは 「DPA 別表」) にも、「クラウド・サービス」およびそのオプション (処理対象の「コンテンツ」の種類、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ついての仕様書に関連) に関する追加的なデータ保護情報が記載されています。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、DPA が適用されます。

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

3. サービス・レベルおよびテクニカル・サポート

3.1 サービス・レベル・アグリーメント

IBM は、以下の可用性のサービス・レベル・アグリーメント (以下「SLA」といいます。) をお客様に提供します。IBM は、下表のとおり、「クラウド・サービス」の累積的な可用性に基づき、適用しうる最大の補償を適用します。「可用性」は、契約月における分単位の総時間数から、契約月における「サービス・ダウン」の分単位の総時間数を差し引き、それを契約月における分単位の総時間数で除することにより算出され、結果はパーセントで表します。「サービス・ダウン」の定義、請求のプロセス、サービスの可用性の問題に関して IBM に連絡する方法については、IBM の SaaS サポートの概要 (https://www.ibm.com/software/support/saas_support_overview.html) に掲載されています。

可用性	クレジット (月額サブスクリプション料金のパーセント*)
99.9% 未満	2%
99.0% 未満	5%
95.0% 未満	10%

*サブスクリプション料金は、請求対象月に関して約定した料金です。

3.2 テクニカル・サポート

「クラウド・サービス」のテクニカル・サポート (サポート窓口の連絡先情報、重大度レベル、サポート利用可能時間、応答時間、その他のサポート情報およびサポート処理など) を参照するには、IBM サポート・ガイド (https://www.ibm.com/support/home/pages/support-guide/) の「クラウド・サービス」を選択します。

4. 料金

4.1 課金単位

「クラウド・サービス」の課金単位は、「取引文書」に記載されます。

以下の課金単位が本「クラウド・サービス」に適用されます。

- 「エンゲージメント」とは、「クラウド・サービス」に関するプロフェッショナル・サービスまたはトレーニング・サービスです。
- 「1 秒あたりのイベント」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、特定のイベントの 1 秒あたりの発生回数をいいます。
- 「1 秒あたりのフロー」とは、「クラウド・サービス」が管理または処理するフローの 1 秒あたりの数をいいます。「フロー」とは、2 つのホスト間の通信記録です。同一のソース 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、1 つの「フロー」記録として結合されます。
- 「アセット」とは、「クラウド・サービス」がアクセスまたは管理する、一意に識別される価値のある有形のリソースまたは項目をいいます。

5. 追加条件

2019 年 1 月 1 日よりも前に締結されるクラウド・サービス契約 (または同等のクラウド基本契約) については、https://www.ibm.com/acs に掲載されている条件を適用します。

5.1 イネーブリング・ソフトウェア

「クラウド・サービス」には以下の「イネーブリング・ソフトウェア」が含まれます。

- 「データ・ゲートウェイ」 – お客様は「データ・ゲートウェイ」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。

6. オーバーライド条件

6.1 セキュリティー・データの使用

以下は、「コンテンツ」、および両当事者間の「クラウド・サービス」の基本条件の「データ保護」項における相反する条件に優先します。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ー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・ハッシュなどです。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。