

IBM QRadar Advisor with Watson

本「サービス記述書」は IBM がお客様に提供するサービスについて規定するものです。お客様とは、会社、その許可ユーザーまたは「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 Advisor with Watson Service

IBM QRadar Advisor with Watson は、コグニティブ分析を QRadar Security Platform まで拡張して、お客様およびセキュリティー・アナリストが速やかに脅威を調査して対応できるようにします。また、Watson for Cyber Security の知識に関するコーパスを活用して、非構造化データ (とりわけ、セキュリティー Web サイト、ブログ、および研究論文を含みます。) を利用し、お客様環境のセキュリティー・インシデントに関連付けます。そうすることにより、隠れた脅威を発見し、洞察を自動化して対応の高速化および意思決定の向上を実現できるように手助けします。QRadar Advisor with Watson により、セキュリティー・アナリストは、セキュリティー・オフENSESを Watson へ送信して脅威の発見を実行し、数十万もの非構造化データ・ソースや構造化データ・ソースの知識ベースを使用し、元のセキュリティー・オフENSESに関連する脅威エンティティーにマッピングしなおります (悪意のあるファイル、疑わしい IP アドレス、非認識エンティティー、およびそれらの関係など)。これは、セキュリティー・オフENSESが既知のマルウェア攻撃に関連するものかどうかを判断する際に特に有益です。その場合、Watson は、いくつかある洞察の中で特に、悪用されたマルウェア、悪用された脆弱性、その脅威の範囲 (影響を及ぼす可能性のある追加のエンドポイントを含みます。) に関するバックグラウンドを提供します。

「クラウド・サービス」では、お客様がアクティブな IBM Security QRadar の導入を行い、お客様がその機能にアクセスできるように当該導入上に「クラウド・サービス」のイネープリング・コードをインストール済みである必要があります。「クラウド・サービス」には、お客様が「クラウド・サービス」に送信できるセキュリティー・オフENSESの照会数 (お客様が資格を有する「毎秒 1000 イベント」ごとに 1 日当たり 15 件の要求という割合) に関する「ソフト制限」が含まれています。当該制限を超えて送信された照会は「クラウド・サービス」で処理されますが、優先順位が下がり、より低速で返されます。

1.2 IBM QRadar Advisor with Watson Trial

IBM QRadar Advisor with Watson Trial (以下「評価版クラウド・サービス」といいます。) は、評価版ベースで IBM QRadar Advisor with Watson の機能を提供します。お客様による「評価版クラウド・サービス」へのアクセスは、取引文書またはその他の文書に記載されている期間を上限とし、その期間の終了時点でお客様のアクセスは終了します。お客様は、評価版の期間中、セキュリティー・オフENSES照会を 1 日当たり最大 5 つのみ送信できます。「評価版クラウド・サービス」は保証適用なしで「現状のまま」提供されるため、お客様は内部テストおよび非実稼働使用のためのみ使用できます。照会に対する応答時間は、現在のトラフィック・レベルに基づき、評価版の期間中は異なる場合があります。

2. セキュリティーの内容

本「クラウド・サービス」は、IBM の「IBM SaaS」に関する「Data Security and Privacy Principles」 (<http://www-03.ibm.com/software/sla/slabd.nsf/sla/dsp> で入手可能) および本セクションの追加条件に従うものとします。IBM の「Data Security and Privacy Principles」が変更される場合であっても、それにより「クラウド・サービス」のセキュリティーのレベルが低下することはありません。

保護対象のデータの処理およびデータの特性により提示されるリスクに対して技術的および組織上のセキュリティー対策が適切であると、お客様がデータ管理者として判断する場合には、本「クラウド・サービス」を使用して、個人データが含まれる厳選されたコンテンツを処理することができます。お客様は、本「クラウド・サービス」ではセンシティブ個人データや追加の規制要件の対象となるデータを保護するためのフィーチャーが提供されないことを認識しています。お客様は、IBM がコンテンツに含まれているデータのタイプを把握していないこと、および「クラウド・サービス」の適合性や適用中のセキュリティー保護に関して評価を行えないことに同意します。

「クラウド・サービス」により、お客様は以下のコンテンツのみを入力、管理できます。以下のコンテンツの一部は、適用されるプライバシー法の下で個人情報(以下「PI」といいます。)とみなされる可能性があります。

- ターゲット/ソース IP アドレス
- URL
- ドメイン
- ファイル・ハッシュ

2.1 セキュリティー・フィーチャーおよび責任

「クラウド・サービス」には、以下のセキュリティー・フィーチャーが実装されています。

「クラウド・サービス」では、IBM ネットワークとおお客様の IBM Security QRadar 導入との間のデータ伝送中にコンテンツを暗号化します。「クラウド・サービス」では、データ伝送を待機中の静止時に、コンテンツの暗号化は行われません。

「クラウド・サービス」では、当該データについてその機能を実行後は、当該入力コンテンツを保持しません。

3. 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、下記に従い、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。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、別個のオフオファリングとして提供されるものではありません。

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 事業上の重要な機能が作動不能である、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に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 利用中にサービスのフィーチャーまたは機能が著しく制限されているか、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することができ、業務に重大な影響が表れていないことを示す。	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依頼。	1 営業日以内	月曜から金曜の営業時間

「クラウド・サービス」のベータ版に参加し、QRadar Platform のバージョン 7.2.7 を現在も使用中のお客様については、テクニカル・サポートに関する一部の問題を解決できない場合があります。かかるお客様は提供可能なテクニカル・サポートをすべて受けるためにバージョン 7.2.8 へアップグレードし、最新のバッチをインストールする必要があります。

4. エンタイトルメントおよび課金情報

4.1 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。

- 「毎秒 100 イベント」**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「証書 (PoE)」または「取引文書」に定める課金期間中に生じる1秒当たりの「イベント」の数(100の単位で切り上げ)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。

5. 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。

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。

6. 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。

「クラウド・サービス」のイネーブリング・ソフトウェアは、IBM Security App Exchange (<https://exchange.xforce.ibmcloud.com/hub> に掲載) からお客様がダウンロードできます。

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。

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。

「クラウド・サービス」のイネーブリング・ソフトウェアは、IBM Security App Exchange (<https://exchange.xforce.ibmcloud.com/hub> に掲載) からお客様がダウンロードできます。

7.3 クラウド・サービスの合法的利用

「クラウド・サービス」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。「クラウド・サービス」の利用は、さまざまな法律または規制に関わる場合があります。これには、プライバシー、データ保護、雇用、電子通信、および電子保管に関連するものが含まれます。「クラウド・サービス」は、合法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「クラウド・サービス」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。お客様は、「クラウド・サービス」の合法的な利用に必要なすべての同意、許可、またはライセンスを取得するか、取得済みであることを表明します。

7.4 クラウド・サービスの有効期限

「クラウド・サービス」の満了または終了の前に、お客様は「クラウド・サービス」について提供された報告機能またはエクスポート機能を使用してデータを抽出することができます。

7.5 セキュリティー・データ

報告作業を含む「クラウド・サービス」の一部として、IBM は、「クラウド・サービス」から収集された情報を匿名化または集約したものを準備し、維持管理します (以下「セキュリティー・データ」といいます)。「セキュリティー・データ」では、下記 (d) に定めるものを除いて、お客様も個人も特定することはありません。お客様は本書において、以下のみを目的として IBM が「セキュリティー・データ」を使用またはコピーできることにさらに同意します。

- a. 「セキュリティー・データ」の公表または配布 (サイバーセキュリティーに関連する集計または分析など)
- b. 製品やサービスの開発または拡張
- c. 社内で、または第三者と共に実施する調査
- d. 確認済みの第三者の攻撃者情報の合法的な共有