# IBM Financial Crimes Insight

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。該当する注文関連文書には、お客様の発注に関する価格の詳細情報および追加の詳細情報が記載されています。

## 1. クラウド・サービス

### 1.1 オファリング

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 Financial Crimes Insight

本「クラウド・サービス」は、Financial Crimes Insight オファーの構築ベースとなる、共通のインフラストラクチャーおよびサービスのセットを提供します。IBM Financial Crimes Insight は、オファリング間で必要な統合を行い、お客様が統合された金融犯罪に関するオファリング・セットを活用できるようにします。

IBM Financial Crimes Insight は、「クラウド・サービス」の「インスタンス」を提供する必須のコンポーネントです。

#### 1.1.2 IBM Financial Crimes Insight Non-Production

この「クラウド・サービス」により、お客様は、クラウド・オファリングとして IBM Financial Crimes Insight Non-Production 機能にアクセスできます。

#### 1.1.3 IBM Financial Crimes Insight BYOL

この「クラウド・サービス」により、お客様は、クラウド・オファリングとして IBM Financial Crimes Insight 機能にアクセスできます。BYOL (Bring Your Own License) オファリングでは、お客様は、関連 IBM プログラムの適切なライセンス資格を事前に取得している必要があります。IBM Financial Crimes Insight BYOL オファリングで必要な「IBM プログラム」は、IBM Cloud Pak for Data Financial Crimes Insight です。

#### 1.1.4 IBM Financial Crimes Insight Non-Production BYOL

この「クラウド・サービス」により、お客様は、クラウド・オファリングとして IBM Financial Crimes Insight Non-Production 機能にアクセスできます。BYOL (Bring Your Own License) オファリングでは、お客様は、関連 IBM プログラムの適切なライセンス資格を事前に取得している必要があります。IBM Financial Crimes Insight Non-Production BYOL オファリングで必要な「IBM プログラム」は、IBM Cloud Pak for Data Financial Crimes Insight for Non-Production Environment です。

#### 1.1.5 IBM Financial Crimes Insight for Entity Research Negative News API

本「クラウド・サービス」は、コグニティブ・コンピューティング・テクノロジーおよび拡張分析を使用して、フィルタリング後にランク付けされた記事の一覧を出力することでエンティティーの潜在的な金融犯罪リスクを明らかにするために、構造化されていないニュースおよびメディアを検索して分析し、優先順位を付けます。このオファリングは、組織が各自のワークフローおよびプロセスを呼び出すか、またはそれらに組み込むための API として提供されます。

#### 1.1.6 IBM Financial Crimes Insight for Entity Research Enrichment API

本「クラウド・サービス」はコグニティブ・コンピューティング・テクノロジーを使用して、組織がエンティティーについて理解を深めるのに役立つ構造化ソースからのデータを集約して、エンティティーまたは顧客の記録を常に最新の状態に保ち、エンティティーの潜在的な金融犯罪リスクを明らかにします。エンティティーには顧客、取引先、またはサプライヤーが含まれる場合があります。このオファリングは、組織が各自のワークフローおよびプロセスを呼び出すか、またはそれらに組み込むための API として提供されます。

## 1.2 オプション・サービス

IBM Financial Crimes Insight または IBM Financial Crimes Insight Non-Production のサブスクリプションに加えて、お客様は、以下の「クラウド・サービス」のうちいずれかに対するサブスクリプションも取得しなければなりません。

### 1.2.1 IBM Financial Crimes Insight for Anti-Money Laundering

IBM Financial Crimes Insight for Anti-Money Laundering (FCI for AML) は拡張分析のレイヤーを適用して、財務活動を監視し、お客様がエンティティーの資金洗浄の傾向を特定できるようにします。人口統計、行動、および関係に関するデータを使用する FCI for AML は、お客様がプロセスを見直して既知のリスクを見つけるのに役立ちます。また、隠れたリスクについて説明可能な洞察を提供することで対象のリスク範囲が広がる場合があります。

### 1.2.2 IBM Financial Crimes Insight for Alert Triage – AML Transaction Monitoring

本「クラウド・サービス」は、アラート・トリアージ手順の円滑化、誤判定の低減、アラート処理の促進、およびエンティティーが負うリスクついて理解を深めることによる意思決定の改善を目的として、過去のケースのデータ、文脈上の証拠に関するデータ集約、および機械学習機能を活用します。本サービスは、お客様の組織の既存のトランザクション監視システムとケース管理システム間に適合する追加的な構成要素です。

### 1.2.3 IBM Financial Crimes Insight for Alert Triage – Transaction List Screening

本「クラウド・サービス」は、構成と拡張が可能な API ベースのパイプラインを使用して、アラートが出た取引を分析することで、既存の制裁スクリーニング・システムを強化します。取引データをクリーンアップし、解析してまとめた後、ヒューリスティックおよびコグニティブ・コンピューティングの手法により処理します。この結果を使って該当項目をスコア化し、誤検知を特定し、参考になるカスタマイズ可能な洞察を返します。

### 1.2.4 IBM Financial Crimes Insight for Entity Research

本「クラウド・サービス」は、エンティティーについて、およびエンティティーと事業を行うことに関連するリスクについて理解を深めること、ならびに KYC (Know Your Customer) に関わるアクティビティーの完了に要する時間を短縮することを目的として、構造化データ・ソースおよび非構造化データ・ソースの関連コンテンツをスクリーニング、抽出、およびリンクするためにコグニティブ・コンピューティング・テクノロジーを活用します。本ソリューションは、さまざまなデータ・ソースの集約により、顧客情報の調査および分析の自動化および標準化を支援します。本サービスの目的は、調査およびデュー・ディリジェンス・アクティビティーの完了を合理化することでお客様のエクスペリエンスを改善することに加えて、KYC レコードの品質を向上させることです。

**お客様は以下の使用許諾オプションから選択できます。**

- IBM Financial Crimes Insight for Entity Research – Enterprise – 「イベント」ごとに、5 つを超える関連当事者の調査が可能です。
- IBM Financial Crimes Insight for Entity Research – Advanced – 「イベント」ごとに、最大 5 つの関連当事者の調査が可能です。
- IBM Financial Crimes Insight for Entity Research – Basic – 「イベント」ごとに、最大 2 つの関連当事者の調査が可能です。

関連当事者とは、第 4.1 項に定められた「親調査」のためのレビューの一部として調査する必要のあるエンティティー (組織または個人) です。一般的に、権限のある署名者、担当者、最終的な受益株主、組織図内の親組織または下部組織がこれに該当します。疑義を避けるため付言すると、関連当事者が個人または関連のあるメンバーの調査が必要なエンティティーの場合には、個人または関連のあるメンバーも関連当事者とみなされます。

### 1.2.5 IBM Financial Crimes Insight for Entity Research with Material Change

本「クラウド・サービス」は、エンティティーについて、およびエンティティーと事業を行うことに関連するリスクについて理解を深めること、ならびに KYC (Know Your Customer) に関わるアクティビティーの完了に要する時間を短縮することを目的として、構造化データ・ソースおよび非構造化デー

タ・ソースの関連コンテンツをスクリーニング、抽出、およびリンクするためにコグニティブ・コンピューティング・テクノロジーを活用します。本ソリューションは、さまざまなデータ・ソースの集約により、顧客情報の調査および分析の自動化および標準化を支援します。本サービスの目的は、調査およびデュー・ディリジェンス・アクティビティーの完了を合理化することでお客様のエクスペリエンスを改善することに加えて、KYC レコードの品質を向上させることです。これには、重大な差異を見つけるためにスケジュールどおりにエンティティーを監視し、アナリストに確認を促すことができる「重大な変更」機能が含まれます。

**お客様は以下の使用許諾オプションから選択できます。**

- IBM Financial Crimes Insight for Entity Research – Enterprise – 「イベント」ごとに、5 つを超える関連当事者の調査が可能です。
- IBM Financial Crimes Insight for Entity Research – Advanced – 「イベント」ごとに、最大 5 つの関連当事者の調査が可能です。
- IBM Financial Crimes Insight for Entity Research – Basic – 「イベント」ごとに、最大 2 つの関連当事者の調査が可能です。

関連当事者とは、第 4.1 項に定められた「親調査」のためのレビューの一部として調査する必要のあるエンティティー (組織または個人) です。一般的に、権限のある署名者、担当者、最終的な受益株主、組織図内の親組織または下部組織がこれに該当します。疑義を避けるため付言すると、関連当事者が個人または関連のあるメンバーの調査が必要なエンティティーの場合には、個人または関連のあるメンバーも関連当事者とみなされます。

### 1.2.6 IBM Financial Crimes Insight for Claims Fraud – Property and Casualty

本「クラウド・サービス」は、組織がデータを分析し、それぞれの顧客によって、医療提供者またはその他のエンティティーによって、および完全調査ライフサイクルおよび成果に関するレポートを管理する目的で、提出される不正な請求に起因するリスクを検知するのに役立ちます。

### 1.2.7 IBM Financial Crimes Insight for Claims Fraud – Investigation

本「クラウド・サービス」は、組織が疑わしいアクティビティーおよび潜在的な不正に関する完全調査ライフサイクルを管理するのに役立ちます。

### 1.2.8 IBM Electronic Communication Surveillance Analytics on Cloud

本「クラウド・サービス」は、金融サービス機関が、さまざまなパターンの疑わしい通信を検知するために、複数のチャネルにわたって従業員の対話データを効果的に分析および監視できるようにするツールです。このツールは、市場における不正行為や市場操作に関連するさまざまなパターンの認識されない行動を検知するのに役立ちます。このツールでは言語処理機能を活用して、テキスト情報を理解したり、文脈ベースで多義用語を区別したりします。このツールでは、通信を分析するために使用できるセンチメント分析機能や情緒分析機能も利用します。これらの機能は、個人の性格特性を推論するために使用することを目的に提供されるものでも、それを推論するものでもありません。この分析は、総合的な推論エンジンに送られます。これは、さまざまな洞察と関連付けたり、リスクの概算をコンプライアンス担当者に提供したりするのに役立ちます。

### 1.2.9 IBM Voice Surveillance Analytics on Cloud

本「クラウド・サービス」は、金融サービス機関が、複数のチャネルにわたって従業員の音声通信を分析、モニターし、疑わしい活動を検知できるようにするツールです。このツールは、文法と言語構造を検知する機械学習を活用することで、人の音声を書き言葉に変換する Speech-to-text テクノロジーを使用します。IBM Voice Surveillance Analytics on Cloud は、対象の音声会話の迅速かつ容易な検索と再生を可能にするために、Speech to Text の出力をテレフォニー・システムによって生成される豊富なメタデータとリンクさせ、話者ダイアライゼーションをテキストに適用します。Speech to Text の出力は、メタデータと共に、明確に定義されたフォーマットでお客様に提供されます。追加的なオプションとして、このツールは、自然言語処理を使用してセマンティック・メタデータをコンテンツから抽出したり、言語分析を使用して話題、トーン、心理および感情を検知することもできます。これらの機能は、個人の性格特性を推論するために使用することを目的に提供されるものでも、それを推論するものでもありませ

ん。音声からテキストへの変換はすべて「メモリー」内で処理され、重複ファイルや重複トランスクリプトの保管を低減します。この処理後、音声データは「クラウド」に一切、保存されません。

### 1.2.10 IBM Complaints Analytics on Cloud

本「クラウド・サービス」により、組織は、クレーム、主張、その他の活動を特定し、集約し、分類できるようになります。本サービスは、拡大しつつある規制上の要求事項に対処するために、新たな問題に対する洞察を提供します。このツールは先進的なアナリティクスを活用して、従来のシステムでは見過ごされた可能性があるクレームを特定して、分析します。お客様のデータ、電子メール、サービス・ノート、ソーシャル・メディアのクレーム、および音声記録などの構造化データおよび非構造化データを取り込むことができます。次にコグニティブ機能を使用して、クレーム・データの集約およびエンリッチメントを行い、システミック・リスクを特定します。また、動的セグメント化および時系列プロファイリングを適用して、変化と動向をモニターし、予測します。

IBM Complaints Analytics on Cloud を使用するためには、お客様は、IBM Electronic Communication Surveillance Analytics on Cloud または IBM Voice Surveillance Analytics on Cloud のいずれかのサブスクリプションも取得しなければなりません。

### 1.2.11 IBM Electronic Communication Surveillance Analytics on Cloud BYOL

この「クラウド・サービス」により、お客様は、クラウド・オファリングとして IBM Electronic Communication Surveillance Analytics on Cloud 機能にアクセスできます。BYOL (Bring Your Own License) オファリングでは、お客様は、関連 IBM プログラムの適切なライセンス資格を事前に取得している必要があります。IBM Electronic Communication Surveillance Analytics on Cloud BYOL オファリングで必要な「IBM プログラム」は、IBM Financial Crimes Insight for Conduct Surveillance Software – Electronic Communication です。

### 1.2.12 IBM Voice Surveillance Analytics on Cloud BYOL

本「クラウド・サービス」により、お客様は、クラウド・オファリングとして IBM Voice Surveillance Analytics on Cloud 機能にアクセスできます。BYOL (Bring Your Own License) オファリングでは、お客様は、関連 IBM プログラムの適切なライセンス資格を事前に取得している必要があります。IBM Voice Surveillance Analytics on Cloud BYOL オファリングで必要な「IBM プログラム」は、IBM Financial Crimes Insight for Conduct Surveillance Software – Voice です。

### 1.2.13 IBM Complaints Analytics on Cloud BYOL

この「クラウド・サービス」により、お客様は、クラウド・オファリングとして IBM Complaints Analytics 機能にアクセスできます。BYOL (Bring Your Own License) オファリングでは、お客様は、関連 IBM プログラムの適切なライセンス資格を事前に取得している必要があります。IBM Complaints Analytics on Cloud BYOL オファリングで必要な「IBM プログラム」は、IBM Financial Crimes Insight for Conduct Surveillance Software – Complaint Analytics です。

## 1.3 アクセラレーション・サービス

### 1.3.1 IBM Financial Crimes Insight Set-up

対応する「クラウド・サービス」が利用できるようにお客様に対してプロビジョニングするためには、以下のセットアップ・サービスが必要になります。

- IBM Financial Crimes Insight for Anti-Money Laundering Set-up
- IBM Financial Crimes Insight for Alert Triage – AML Transaction Monitoring Set-up
- IBM Financial Crimes Insight for Alert Triage – Transaction List Screening Set-up
- IBM Financial Crimes Insight for Entity Research – Enterprise Set-up
- IBM Financial Crimes Insight for Entity Research – Advanced Set-up
- IBM Financial Crimes Insight for Entity Research – Basic Set-up
- IBM Financial Crimes Insight for Entity Research with Material Change – Enterprise Set-up
- IBM Financial Crimes Insight for Entity Research with Material Change – Advanced Set-up
- IBM Financial Crimes Insight for Entity Research with Material Change – Basic Set-up

- IBM Financial Crimes Insight for Entity Research Negative News API Set-up
- IBM Financial Crimes Insight for Entity Research Enrichment API Set-up
- IBM Financial Crimes Insight for Claims Fraud – Property and Casualty Set-up
- IBM Financial Crimes Insight for Claims Fraud – Investigation Set-up
- IBM Surveillance Insight for Financial Services on Cloud Set-up

## 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、以下のリンクの「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、対象となる処理活動、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。DPA は、i) EU 一般データ保護規則 (EU/2016/679) (GDPR)、または ii) http://www.ibm.com/dpa/dpl に記載されているその他のデータ保護法が適用される場合に、その適用範囲に限り、「コンテンツ」に含まれる個人データに適用されます。

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=14BD7780D65B11E99EAFC519926DF897

## 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「クラウド・サービス」のサポート・ハンドブック (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<br>(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・プロセスなど) 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、「個別契約書」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。
- 「インスタンス」は、「クラウド・サービス」の特定の構成への各アクセスを意味します。

- 「イベント」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。
  - IBM Financial Crimes Insight for Anti-Money Laundering において、「イベント」とは、1 暦月内の 1,000 万回の金融取引になります。
  - IBM Financial Crimes Insight for Claims Fraud – Property and Casualty および IBM Financial Crimes Insight for Claims – Investigation において、「イベント」とは「請求」が 1 回発生することをいいます。「請求」とは、カバーされる損失または事象の補償範囲または補償に対する組織への正式要求に関連した一連の指示になります。
  - IBM Financial Crimes Insight for Alert Triage – AML Transaction Monitoring において、「イベント」とは、1 暦月の間に発信元システムから「クラウド・サービス」へ取り込まれる 1 件の個々のアラートまたはイベントをいいます。通常、発信元システムとは、取引モニタリング・システムまたはケース管理システムになります。
  - IBM Financial Crimes Insight for Alert Triage – Transaction List Screening において、「イベント」とは、1 暦月の間に発信元システムから「クラウド・サービス」へ取り込まれる最大 1,000 件の個々のアラートをいいます。通常、発信元システムとは、取引モニタリング・システムまたはケース管理システムになります。
  - IBM Financial Crimes Insight for Entity Research および IBM Financial Crimes Insight for Entity Research with Material Change において、「イベント」とは、1 暦月の間に「クラウド・サービス」によって処理される親調査 (同一の検索の繰り返しを含みます。) をいいます。親調査とは、別の調査に子として関連付けられていないレコードになります。子とは、親調査の対象にはならない関連当事者 (第 1.2.5 項に記載) になります。
- 「適格参加者」とは、「クラウド・サービス」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個人またはエンティティーです。
- 「アイテム」とは、「クラウド・サービス」の利用により管理、処理される、または「クラウド・サービス」の利用に関連する特定のアイテムが 1 回発生することをいいます。
  - IBM Voice Surveillance Analytics on Cloud において、「アイテム」とは、1 暦日の間に「クラウド・サービス」で処理される 1 時間の「音声ストリーム」です。「音声ストリーム」は、リアルタイムまたは録音形式のいずれかの音声通信を取り込んだものになります。
- 「API 呼び出し」は、プログラマブル・インターフェースによる「クラウド・サービス」の呼び出しです。
- 「エンティティー ID」は、「クラウド・サービス」内で識別されるエンティティーの固有の識別子です。

## 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・サービス契約書 (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 サポート・プログラム

IBM Financial Crimes Insight および IBM Financial Crimes Insight Non-Production には、クラウド環境でデプロイされる特定のプログラム (以下「サポート・プログラム」といいます。) へのアクセスが含まれます。お客様は、不正、金融犯罪、および不適切な支払いを特定して阻止するか、そのいずれかを行うために措置に反論するか、その他の措置を講じる目的でのみ、これらの「サポート・プログラム」を使用できます。

#### 5.1.1 使用制限 – 特定のサポート・プログラムに関するもの

以下の「サポート・プログラム」は以下の制限に基づいて利用可能です。

- IBM Watson Studio – Entitlement: 5 人の「同時ユーザー」
- IBM Watson Machine Learning – Entitlement: 50 個の「モデル」

- IBM Openscale – Entitlement: 50 個の「モデル」
- IBM SPSS Modeler Premium – Entitlement: 4 人の「許可ユーザー」
- IBM SPSS Statistics Standard – Entitlement: 4 人の「許可ユーザー」
- Watson Explorer Advanced Edition – Entitlement: 以下の定義どおり「X ギガバイト」あたり。

  お客様は以下を分析することができます。

  - 「非アナリティクス・コレクション」で使用するための「クラウド・サービス」のリポジトリーに保管されているすべての「コンテンツ」
  - 「非アナリティクス・コレクション」で使用するための「クラウド・サービス」のリポジトリーに保管されていない、最大 10 ギガバイトの「コンテンツ」
  - 「アナリティクス・コレクション」で使用するための「クラウド・サービス」のリポジトリーに保管されている、100 ギガバイトの「コンテンツ」

    「アナリティクス・コレクション」とは、Watson Explorer アノテーションの「管理コンソール」で作成されたコレクション、または Watson Explorer Content Analytics の「管理コンソール」内で、または「コンテンツ・アナリティクス」もしくは「アナリティクス」のタイプの API 経由で作成されたコレクションをいいます。

    「非アナリティクス・コレクション」には、「プログラム・クラウド・サービス」で分析されたすべてのその他のコンテンツが含まれます。
- IBM InfoSphere DataStage – IBM InfoSphere DataStage and QualityStage Designer Entitlement: 2 人の「許可ユーザー」
- IBM Operational Decision Manager – Entitlement: 100 万件の「月間のルールに基づく意思決定」および 1,000 件の「月間の管理対象の意思決定に関する成果物」

**使用許諾に関する定義**

a. 「同時ユーザー」とは、ある特定の時点で「サポート・プログラム」にアクセスしている 1 人のユーザーをいいます。当該ユーザーが複数回、「サポート・プログラム」に同時アクセスしているかどうかに関わらず、当該ユーザーは、1 人の「同時ユーザー」としてカウントします。

b. 「モデル」とは、「サポート・プログラム」でのシミュレーション、説明、予測作成のために使用される基礎となるデータまたはデータ生成プロセスに関する、数学モデルまたはアルゴリズムをいいます。

c. 「許可ユーザー」とは、直接または間接のいかなる方法においても (例えば、多重化プログラム、デバイスまたはアプリケーション・サーバーを通じて)「サポート・プログラム」へのアクセス権限を付与されている特定のユーザーを指します。

d. 「ギガバイト (GB)」は、「サポート・プログラム」によって処理されるか、「サポート・プログラム」において分析、使用、保管、または構成される、2 の 30 乗バイトのデータです。

e. 「月間のルールに基づく意思決定」は、任意の 1 暦月の間に「サポート・プログラム」によって実行または処理されるルール実行サーバーからルールセットを呼び出すことで生じる結果をいいます。

f. 「月間の管理対象の意思決定に関する成果物」とは、任意の 1 暦月の間に「サポート・プログラム」で管理されるオブジェクトをいいます。

## 5.2 IBM Financial Crimes Insight BYOL に適用される条件

BYOL (Bring Your Own License) オファリングでは、お客様は、下表に明記された関連 IBM プログラムの適切なライセンス資格を事前に取得している必要があります。BYOL SaaS に対するお客様の使用許諾は、下記の比率で、関連 IBM プログラムに対するお客様の使用許諾を超えることはできません。

BYOL オファリングには、関連 IBM プログラムのサブスクリプション & サポート (S&S) は含まれていません。お客様は、関連 IBM プログラムに対する適用可能な (1) ライセンス資格、および (2) S&S を予め取得していることを表明するものとします。BYOL オファリングのサブスクリプション期間中、お客様

は、BYOL オファリングの使用許諾と併せて使用する IBM プログラムの使用許諾に対する最新の S&S を維持する必要があります。関連 IBM プログラムを使用するためのお客様のライセンス、または関連 IBM プログラムのお客様の S&S のいずれかが終了した場合、お客様の BYOL オファリングを使用する権利は終了します。

お客様は、以下の期間 (以下「同時使用期間」といいます。) にわたって、BYOL オファリングのお客様による使用と同時に、関連する IBM プログラムを導入するために BYOL オファリングの使用に適用される、関連する IBM プログラムの使用許諾を引き続き使用できます。サブスクリプション期間が 3 年未満のお客様については、BYOL オファリングの初期サブスクリプションをお客様が開始してから 90 日以内。サブスクリプション期間が 3 年以上のお客様については、BYOL オファリングの初期サブスクリプションをお客様が開始してから 1 年以内。「同時使用期間」の終了後、BYOL オファリングを使用する間、BYOL オファリングの使用に適用される関連 IBM プログラムに対するお客様の使用許諾は中断され、お客様はそれ以降、当該使用許諾を使用して、関連 IBM プログラム (規定された例外の対象) をデプロイすることはできません。

下表は、規定された対応する使用許諾に基づいた BYOL オファリングの使用に必要な関連 IBM プログラムの使用許諾の比率の概要を説明したものです。お客様が BYOL オファリングを取得し、BYOL オファリングを使用する間、BYOL オファリングの使用に適用される関連 IBM プログラムに対するお客様の使用許諾は中断され、お客様はそれ以降、当該使用許諾を使用して、関連 IBM プログラム (規定された例外の対象) をデプロイすることはできません。

| 関連 IBM プログラム | BYOL オファリング | 比率 n/m* |
|---|---|---|
| IBM Cloud Pak for Data Financial Crimes Insight | IBM Financial Crimes Insight BYOL | 比率: 1 インストール / 1 インスタンス |
| IBM Cloud Pak for Data Financial Crimes Insight for Non-Production Environment | IBM Financial Crimes Insight Non-Production BYOL | 比率: 1 インストール / 1 インスタンス |
| IBM Financial Crimes Insight for Conduct Surveillance Software – Electronic Communication | IBM Electronic Communication Surveillance Analytics on Cloud BYOL | 累積比率:<br>ティア 1 (1 〜 100 RVU):<br>● 1 RVU / 1 適格参加者<br>ティア 2 (101 〜 235 RVU):<br>● 0.9 RVU / 1 適格参加者<br>ティア 3 (236 〜 435 RVU):<br>● 0.8 RVU / 1 適格参加者<br>ティア 4 (436 〜 585 RVU):<br>● 0.6 RVU / 1 適格参加者<br>ティア 5 (586 〜 835 RVU):<br>● 0.5 RVU / 1 適格参加者<br>ティア 6 (836 〜 1,135 RVU):<br>● 0.4 RVU / 1 適格参加者<br>ティア 7 (1,136+ RVU):<br>● 0.3 RVU / 1 適格参加者 |

| 関連 IBM プログラム | BYOL オファリング | 比率 n/m* |
|---|---|---|
| IBM Financial Crimes Insight for Conduct Surveillance Software – Voice | IBM Voice Surveillance Analytics on Cloud BYOL | 累積比率:<br>ティア 1 (1 ～ 100 RVU):<br>● 1 RVU / 1 アイテム<br>ティア 2 (101 ～ 235 RVU):<br>● 0.9 RVU / 1 アイテム<br>ティア 3 (236 ～ 435 RVU):<br>● 0.8 RVU / 1 アイテム<br>ティア 4 (436 ～ 585 RVU):<br>● 0.6 RVU / 1 アイテム<br>ティア 5 (586 ～ 835 RVU):<br>● 0.5 RVU / 1 アイテム<br>ティア 6 (836 ～ 1,135 RVU):<br>● 0.4 RVU / 1 アイテム<br>ティア 7 (1,136+ RVU):<br>● 0.3 RVU / 1 アイテム |
| IBM Financial Crimes Insight for Conduct Surveillance Software – Complaint Analytics | IBM Complaints Analytics on Cloud BYOL | 累積比率:<br>ティア 1 (1 ～ 100 RVU):<br>● 5 RVU / 1 エンティティー ID<br>ティア 2 (101 ～ 235 RVU):<br>● 4.5 RVU / 1 エンティティー ID<br>ティア 3 (236 ～ 435 RVU):<br>● 4 RVU / 1 エンティティー ID<br>ティア 4 (436 ～ 585 RVU):<br>● 3 RVU / 1 エンティティー ID<br>ティア 5 (586 ～ 835 RVU):<br>● 2.5 RVU / 1 エンティティー ID<br>ティア 6 (836 ～ 1,135 RVU):<br>● 2 RVU / 1 エンティティー ID<br>ティア 7 (1,136+ RVU):<br>● 1.5 RVU / 1 エンティティー ID |

* 「比率 n/m」は、関連 IBM プログラムに対して示された測定基準の使用許諾数ごと (以下「n」といいます。) に対して、お客様が当該使用許諾を、BYOL オファリングに対して示された測定基準について記載された数 (以下「m」といいます。) の使用許諾に適用できることをいいます。関連 IBM プログラムから BYOL オファリングへの変換の結果が整数にならない場合、最も近い整数に切り上げます。

**例 1:**

適格参加者 (EPS) に対して 710 RVU

(IBM Trade Surveillance Analytics および IBM Electronic Communication Surveillance Analytics に適用可能)

ティア 1: 710>100 の場合、100/1 = 100 EPS

ティア 2: 710>235 の場合、(235-100)/.9 = +150 EPS

ティア 3: 710>435 の場合、(435-235)/.8 = +250 EPS

ティア 4: 710>585 の場合、(585-435)/.6 = +250 EPS

ティア 5: 710>835 の場合、これはないので、(710-585)/.5 = +250 EPS

合計 EPS: 100 + 150 + 250 + 250 + 250 = 1000 EPS

**例 2:**

250 RVU (100,000 パック) から エンティティー ID (500,000 パック)

(IBM Complaints Analytics に適用可能)

ティア 1: 250>100 の場合、100/5 = 20 エンティティー ID

ティア 2: 250>235 の場合、(235-100)/4.5 = +30 エンティティー ID

ティア 3: 250>435 の場合、これはないので、(250-235)/4 = +3.75 エンティティー ID

合計 EPS: 20 + 30 + 3.75 = 53.75 エンティティー ID、54 エンティティー ID に切り上げ

チェック: 250 RVU = 269 リソース * 100,000 パック・サイズ オンプレミス / 500,000 パック・サイズ SaaS = 53.75、54 エンティティー ID に切り上げ

## 5.3 第三者のコンテンツ

お客様は、本書に記載された「クラウド・サービス」の一部として生成されたレポートで取得および参照されている検索結果には、第三者が所有するデータまたは「コンテンツ」が含まれている場合があること、および IBM がかかる「検索結果」や「コンテンツ」に関わるライセンスやその他の権利を販売したり、提供したりしないことを了承します。お客様は、お客様、またはお客様の代理人として IBM がかかる「検索結果」を使用、所有、保持、処理、または複製もしくは改作する場合に、かかる「検索結果」に適用される法律に基づき必要に応じて、かかるすべてのライセンス、権利および許可を該当する第三者から取得する全責任を負い、本書に記載された「クラウド・サービス」を使用する前にそれらを取得するものとすることに同意します。お客様は、本書の「クラウド・サービス」に関連して、IBM および IBM の関連会社、ならびにいずれかの請負業者に、お客様の代わりに第三者のデータ・ソースにアクセスする、当該データ・ソースを複製、改作、またはその他の方法で処理する権限を付与します。本第 5.3 項において、「コンテンツ」は、お客様またはお客様の許可ユーザーが提供、アクセス権限を付与、または「クラウド・サービス」に入力する、あらゆる著作物、データ、イメージ、ソフトウェアもしくは情報で構成されるものとします。

## 5.4 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。カスタム・データ抽出サービスは、別途契約に基づいて提供されます。

「クラウド・サービス」の満了日または終了日から 30 日以内にお客様からサポート要求を受け取った場合、IBM はお客様のコンテンツの電子コピーをネイティブ・アプリケーション形式でお客様に返却します。