IBM クラウド・サービス記述書

IBM OpenPages GRC on Cloud

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、以下に記載されていますが、一部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」およびお客様が受領し「クラウド・サービス」の開始日および期間、ならびに請求の開始時期を確認する「証書 (PoE)」で構成されます。

1.1 IBM OpenPages GRC on Cloud

IBM OpenPages GRC on Cloud (必須コンポーネント) は、企業全体でリスクおよびコンプライアンスのイニシアチブを特定、管理、監視、報告する機能を提供する Operational Risk Management の標準構成を提供します。これは、RCSA (リスクと統制の自己評価)、損失イベント、シナリオ分析、外部損失、および KRI (重要リスク評価指標) を含む、すべてのリスク・データをまとめて単一のモジュールに統合するために使用することができます。

Operational Risk Management の機能には以下が含まれます。

- 主要機能。
  (1) リスクの特定、測定、および軽減を可能にする。
  (2) 内部統制のテストおよび記録を可能にする。
- 損失イベント。これにより以下のアクティビティーが可能になります。
  (1) 営業損失を招く恐れがある内部イベントおよび外部イベントの両方を追跡、評価、管理する。
  (2) 営業損失に関連するマルチ・インパクト・イベントおよび回復を管理する。
- 外部損失イベントは、シナリオ分析、ベンチマーキング、およびレポート作成のために、損失データを、IBM Algo FIRST、Operational Risk data eXchange Association (ORX)、および Operational Risk Consortium (ORIC) 損失データベース (別個のサブスクリプションが必要) から IBM OpenPages Operational Risk Management にインポートする機能を提供します。損失データを、分析ツールまたは資本配分アプリケーションにエクスポートすることもできます。
- KRI。リスクの概況や傾向の存在または状態を潜在的に示すパフォーマンス・メトリックを追跡するために使用することができます。
- シナリオ分析。特定の種類のリスク、とりわけ低頻度、大規模イベントを特定および測定するために使用できる評価手法です。
- 報告、監視、および分析。
- IBM SoftLayer クラウドの実装。

1.2 IBM OpenPages GRC Non-Production Instance on Cloud

IBM OpenPages GRC Non-Production Instance on Cloud は、社内での開発およびテスト作業のための、「クラウド・サービス」の非実稼働インスタンスを提供します。

1.3 IBM OpenPages GRC Data Storage on Cloud

IBM OpenPages GRC Data Storage on Cloud (必須コンポーネント) は、「クラウド・サービス」のお客様のインスタンスのために、GRC データのストレージを提供します。ストレージは、150 ギガバイトを割り当て単位として販売されます。

1.4 IBM OpenPages GRC Administrator User on Cloud

IBM OpenPages GRC Administrator User on Cloud (少なくとも 1 つは必須) のユーザーは、すべての管理機能および「クラウド・サービス」の Operational Risk Management 機能に対するアクセスを許可されます。

1.5 IBM OpenPages Operational Risk Management User on Cloud

IBM OpenPages Operational Risk Management User on Cloud のユーザーは、上記の Operational Risk Management 機能との対話のみを許可されます。

1.6 IBM OpenPages GRC Operational Risk Management Jump Start on Cloud

IBM OpenPages GRC Operational Risk Management Jump Start on Cloud (必須コンポーネント) は、「クラウド・サービス」の初回の導入に関するサービスを提供します。これには、プロジェクトの計画、保守、管理、および実証された手法の検討に関する初回の指導および支援が含まれます。

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、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 には、インフォメーション・セキュリティー・チームがあります。IBM セキュリティー・ポリシーおよび基準については 1 年ごとに審査し、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。クライアント・データへのアクセス、およびホスティング環境へのデータ転送またはホスティング環境からのデータ転送は、すべて記録されます。本「クラウド・サービス」をサポートする IBM データ・センター内では、WIFI の使用は禁止されています。

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、実施前に 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・バッジのみを所有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、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 1 年ごとに実施します。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 1 年ごとに受講します。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 1 年ごとに自身の業務目標および責任について再認識します。

3. サービス・レベル・コミットメント

IBM は、「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。お客様は、SLA が、お客様に対する保証とならないことを了承します。

3.1 定義

a. 「可用性クレジット」とは、IBM が検証した「請求」に対して提供する救済措置をいいます。「可用性クレジット」は、返金または「クラウド・サービス」のサブスクリプション料金の将来の請求額から割り引く形で適用されます。

b. 「請求」とは、SLA に基づいて、お客様が IBM に対して提出する、「契約月」中に「サービス・レベル」が満たされていない旨の主張をいいます。

c. 「契約月」とは、その月の初日の午前 12 時 (米国東部標準時) から当該月の末日の午後 11 時 59 分 (米国東部標準時) までを基準とする期間における各 1 か月をいいます。

d. 「ダウン時間」とは、「クラウド・サービス」を処理する実稼働システムが停止し、許諾を取得しているお客様のユーザーが、あらゆる点で「クラウド・サービス」を利用できなくなる期間をいいます 「ダウン時間」には、「クラウド・サービス」が以下のいずれかに起因して利用できなくなった場合の期間は含まれません。

   (1) 保守のための定期的な停止または発表された停止。

   (2) IBM の管理の及ばない事象または原因 (例: 自然災害、インターネット障害、緊急保守等)。

   (3) お客様のアプリケーション、装置もしくはデータ、または第三者のアプリケーション、装置もしくはデータに関する問題。

   (4) 「クラウド・サービス」にアクセスするための必要なシステム構成およびサポートされているプラットフォームの要件をお客様が満たさない場合。

   (5) IBM がお客様またはお客様に代わる第三者が IBM に提供する設計、仕様、または指示に従った場合。

e. 「事象」とは、「サービス・レベル」が満たされない原因となる状況または一連の状況をいいます。

f. 「サービス・レベル」とは、IBM が本 SLA において提供する「サービス」のレベルを評価するための、以下に規定する基準をいいます。

3.2 可用性クレジット

a. 「請求」を提出するには、お客様は、「事象」ごとに、かかる「事象」がお客様の「クラウド・サービス」の利用に影響を与えていることをお客様が最初に認識してから 24 時間以内に、IBM テクニカル・サポート・ヘルプデスクに重要度 1 のサポート・チケット (以下の「テクニカル・サポート」の項に定義されています。) を記録しなければなりません。お客様は「事象」に関するす

べての必要な情報を提供し、「事象」の分析および解決につき IBM を合理的に支援しなければなりません。

b. お客様は、お客様の「可用性クレジット」の「請求」を、「請求」が生じた「契約月」の末日から 3 営業日以内に提出しなければなりません。

c. 「可用性クレジット」は、「ダウン時間」が最初に影響を与えたことがお客様により報告された時刻から測定されるダウン時間に基づいて決定されます。IBM は、有効な各「請求」に対して、適用可能な「可用性クレジット」の最高額を、下表に示した各「契約月」において達成した「サービス・レベル」に基づいて適用します。同「契約月」中における同「事象」に対する「可用性クレジット」は、重複して適用されません。

d. 各「契約月」に支払われた「可用性クレジット」の合計額は、いかなる状況においても、お客様が「クラウド・サービス」に対して IBM に支払った年額料金の 12 分の 1 の 10% を超えないものとします

3.3 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	可用性クレジット (「請求」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)
< 98%	2%
< 97%	5%
< 93%	10%

「可用性」は、以下のとおり算出されます。 (a) 「契約月」における分単位の総時間数 から、(b) 「契約月」における「ダウン時間」の分単位の総時間数を控除し、それを (c) 「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。

例: 「契約月」における総「ダウン時間」900 分

$$\frac{\text{30 日の「契約月」における合計 43,200 分 − 「ダウン時間」900 分 = 42,300 分}}{\text{合計 43,200 分}} = \text{97.9\% の「達成したサービス・レベル」に対する 2\% の「可用性クレジット」}$$

3.4 本 SLA に関するその他の情報

本 SLA は、IBM のお客様のみが利用可能であり、「クラウド・サービス」に関するお客様のユーザー、ゲスト、参加者および許可された招待客によって行われる請求、ならびに、IBM が提供する β 版またはトライアル・サービスには適用されません。SLA は、実稼働使用である「クラウド・サービス」にのみ適用します。SLA は、非実稼働環境 (テスト、災害復旧、品質保証、または開発環境を含みますが、これらに限定されません。) には適用されません。

4. ライセンスおよび課金情報

4.1 課金単位

「クラウド・サービス」は、「注文関連文書」に定める以下の課金単位のいずれかに基づいて利用することができます。

a. 「許可ユーザー」は、「クラウド・サービス」を取得する際の課金単位です。お客様は、何らかの手段により直接または間接的に (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・サーバーを経由して) 「クラウド・サービス」へのアクセスを与えられた特定の「許可ユーザー」ごとに、個別に専用の使用許諾を取得する必要があります。お客様の「注文関連文書」に定める課金期間中に「クラウド・サービス」へのアクセスを与えられた「許可ユーザー」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。

b. 「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使用許諾を取得するものとします。

c. 「ギガバイト」は、「クラウド・サービス」を取得する際の課金単位です。「ギガバイト」とは、2 の 30 乗バイトのデータとして定義されます (1,073,741,824 バイト)。お客様の「注文関連文書」に定める課金期間中に「クラウド・サービス」によって処理される「ギガバイト」の総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。

d. 「インスタンス」は、「クラウド・サービス」を取得する際の課金単位です。「インスタンス」とは、特定の構成の「クラウド・サービス」へのアクセスです。「注文関連文書」に規定されている課金期間中にアクセスおよび使用が可能となる「クラウド・サービス」の各「インスタンス」のために十分な使用許諾を取得するものとします。

4.2 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。

4.3 セットアップ料金

標準的なセットアップ・サービスおよびそれらに適用される料金は、IBM OpenPages Operational Risk Management Jump Start on Cloud オファリングにより定められます。

追加の構成またはサービスが必要なお客様は、補足の「作業指示書」により IBM の OpenPages GRC on Cloud サービスを契約する必要があります。

4.4 1 か月に満たない期間の料金

「1 か月に満たない期間の料金」は、日割りで計算されます。「1 か月に満たない期間の料金」は、IBM がお客様に対して「クラウド・サービス」オファリングへのアクセスが可能になったことを通知した日から開始し、その月の残日数に基づき計算されます。

4.5 超過料金

課金期間中のお客様の「クラウド・サービス」の実際の利用が、「注文関連文書」の「PoE」部分に記載される使用許諾範囲を超える場合には、お客様は、「注文関連文書」の規定に従い、その超過分について請求されます。

5. 期間および更新オプション

5.1 期間

「クラウド・サービス」の期間は、「注文関連文書」に規定されるお客様が「クラウド・サービス」にアクセス可能となったことを、IBM がお客様に通知した日に開始します。「注文関連文書」の「PoE」部分で、期間の正確な開始日と終了日を確認します。お客様は、期間中、IBM または「IBM ビジネス・パートナー」にお問い合わせいただくことで、お客様の「クラウド・サービス」の利用レベルを上げることができます。IBM は、「注文関連文書」でその利用レベルの変更を確認します。

5.2 クラウド・サービス期間の更新オプション

お客様の「注文関連文書」では、以下のいずれかの期間を指定して、期間満了時に「クラウド・サービス」を更新するか否かが規定されます。

5.2.1 自動更新

お客様の「注文関連文書」に、お客様の更新は自動更新と記載されている場合、お客様は、「注文関連文書」に規定されている期間の有効期間満了日の少なくとも 90 日前までに、書面による要求により、期間満了となる「クラウド・サービス」期間を終了させることができます。IBM または「IBM ビジネス・パートナー」が、有効期間満 了日 までにかかる終了通知を受領していない場合、期間満了となる期間は 1 年間、または「PoE」に規定される当該更新前の期間と同じ期間のいずれかで自動更新されます。

5.2.2 請求の継続

「注文関連文書」に、お客様の請求は継続すると付記されている場合、お客様は期間終了後も引き続き「クラウド・サービス」に対するアクセス権を有するものとし、「クラウド・サービス」の利用に対して継続的に請求が行われます。「クラウド・サービス」の利用を中断し、継続的な請求プロセスを停止するためには、お客様は、90 日前までに、IBM または「IBM ビジネス・パートナー」にお客様の「クラウド・サービス」の解約を要請する通知を書面で行う必要があります。お客様のアクセスの解約により、お客様には解約が効力を生じる月内の未処理のアクセス料金が請求されます。

5.2.3 更新必要

「注文関連文書」に、お客様の更新タイプは「終了」であると付記されている場合、「クラウド・サービス」は期間満了時に終了し、お客様の「クラウド・サービス」へのアクセスは削除されます。終了日以降も「クラウド・サービス」の利用を継続するには、お客様は、お客様の IBM 営業担当員または「IBM ビジネス・パートナー」に対して発注し、新規の「サブスクリプション期間」を購入する必要があります。

6. テクニカル・サポート

「クラウド・サービス」の期間中に「クラウド・サービス」に対して提供されるテクニカル・サポートは、http://www-01.ibm.com/software/support/acceleratedvalue/SaaS_Handbook_V18.pdf または IBM が提供する後継の URL に定めます。テクニカル・サポートは「クラウド・サービス」に含まれ、別個のオファリングとして提供されるものではありません。

7. 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。

8. 追加情報

8.1 データ収集

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上記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。

8.2 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。

8.3 非実稼働 (Non-Production) に関する制限

「クラウド・サービス」が「非実稼働」と指定されている場合、その「クラウド・サービス」は、お客様の社内での非実稼働活動に対してのみ使用することができます。この活動には、テスト、パフォーマンス調整、障害診断、内部ベンチマーキング、ステージング、品質保証活動、または公開されたアプリケーション・プログラミング・インターフェースを使用して行われる「クラウド・サービス」に対する内部使用の追加機能もしくは拡張機能の開発などが含まれますが、これらに限定されるものではありません。お客様は、「クラウド・サービス」のいかなる部分も、実稼働に関する適切な使用許諾を取得せずに、その他の目的で利用することはできません。

8.4 法令遵守に関する無保証

「クラウド・サービス」は、お客様が法律、規制、規格または慣行に基づく遵守義務を満たすことを支援するために使用することできます。「クラウド・サービス」が提供する指示、推奨使用法またはガイダンスは、法律上、会計上、またはその他の専門的な助言ではないため、お客様はお客様自身で法律上またはその他の専門的な助言を取得するようにしてください。お客様は、お客様とお客様の活動が適用される法律、規制、規格、および慣行に従う一切の責任を負うものとします。「クラウド・サービス」の使用は、法律、規制、規格または慣行に適合することを保証するものではありません。

さらに、「クラウド・サービス」はお客様を支援するツールであり、第三者に助言を行う場合や、投資その他の事業およびリスク管理について決定を下す場合に、お客様の経営陣および従業員のスキル、判断、および経験の代わりとなるものではないことを、お客様は了承します。お客様は、「クラウド・サービス」の利用による結果の責任を負うものとします。

8.5 第三者の Web サイトまたはその他のサービスへのリンク

お客様または「クラウド・サービス・ユーザー」が、「クラウド・サービス」にリンクされた、または「クラウド・サービス」からアクセス可能な第三者の Web サイトまたはその他のサービスに「コンテンツ」を送信する場合、お客様および「クラウド・サービス・ユーザー」は「コンテンツ」の当該送信を可能にするためのすべての同意を IBM に提供するものとします。ただし、かかる送信は、お客様と第三者の Web サイトまたはサービスの間でのみ行われるものとします。IBM は、かかる第三者のサイト、サービス、またはデータに対していかなる保証または表明もせず、また、かかる第三者のサイト、サービス、またはデータの品質について一切責任を負いません。

8.6 第三者の利益のための使用に関する制限

お客様は、IBM が書面により別段の合意をした場合を除き、「クラウド・サービス」またはそのコンポーネント (「クラウド・サービス」により作成される出力データおよびレポートを含みますが、これらに限定されません。) を、サービス・ビューロー、ホスティング・サービスまたはその他の営利目的の情報技術サービスを第三者に提供するために使用することはできません。

8.7 個人医療情報取り扱いの禁止

「クラウド・サービス」は、HIPAA に準拠するよう設計されていないため、「個人医療情報」の送信や保管に使用することはできません。