

IBM Cloud Integrated Analytics Environment

ご利用条件 (以下「ToU」といいます。) は、本「IBM ご利用条件 – SaaS 特定オファリング条件」 (以下「SaaS 特定オファリング条件」といいます。)、および以下の Web サイトでご覧いただける「IBM ご利用条件 – 一般条件」 (以下「一般条件」といいます。) で構成されています (URL:<http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/>)。

「SaaS 特定オファリング条件」と「一般条件」の規定に矛盾がある場合、「SaaS 特定オファリング条件」が優先して適用されるものとします。「IBM SaaS」の注文、そのアクセスまたは利用により、お客様は「ToU」に同意したものとみなされます。

「ToU」には、「IBM パスポート・アドバンテージのご契約条件」、「IBM パスポート・アドバンテージ・エクスペリエンスのご契約条件」、または「IBM SaaS 特定オファリングのご契約条件」のうち該当する契約条件 (以下「本契約」といいます。) が適用され、これらと「ToU」を合わせて完全な合意として成立します。

1. IBM SaaS

以下の「IBM SaaS」オファリングに、これらの「SaaS 特定オファリング条件」が適用されます。

- IBM Cloud Integrated Analytics Environment
- IBM Cloud Integrated Analytics VPN Connectivity
- IBM Cloud Integrated Analytics Standard Security Appliance
- IBM Cloud Integrated Analytics Enterprise Security Appliance
- IBM Cloud Integrated Analytics Extra Small Server
- IBM Cloud Integrated Analytics Small Server
- IBM Cloud Integrated Analytics Medium Server
- IBM Cloud Integrated Analytics Large Server
- IBM Cloud Integrated Analytics SAN Storage

2. 課金単位

「IBM SaaS」は、「取引文書」で規定された以下の課金単位のいずれかに従って販売されます。

- 「**インスタンス**」は、「IBM SaaS」を取得する際の課金単位です。「インスタンス」とは、「IBM SaaS」の特定の構成へのアクセスを意味します。お客様の「証書 (PoE)」または「取引文書」に定める課金期間中にアクセスおよび利用することが可能な「IBM SaaS」の「インスタンス」ごとに十分な使用許諾を取得しなければならないものとします。
- 「**ギガバイト**」は、「IBM SaaS」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「PoE」または「取引文書」に定める課金期間中に「IBM SaaS」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しなければならないものとします。

3. 料金および課金

「IBM SaaS」に対する料金は、「取引文書」に記載されます。

3.1 1 か月に満たない期間の料金

「取引文書」に記載された 1 か月に満たない期間の料金は、按分にて算定される場合があります。

4. 期間および更新オプション

「IBM SaaS」の期間は、「PoE」に記述されるとおり、「IBM SaaS」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、「IBM SaaS」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、「IBM SaaS」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、「IBM SaaS」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。「IBM SaaS」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。

5. テクニカル・サポート

「IBM SaaS」のテクニカル・サポートが、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 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を規定する IBM Software as a Service Support Handbook を提供します。テクニカル・サポートは「IBM SaaS」で提供されるものであり、個別のオファリングとして利用でき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り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 サービス事業機能またはサービスの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

6. 「IBM SaaS」オファリングの追加条件

6.1 共通事項

お客様は、IBM が報道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「IBM SaaS」の利用者として公に言及できることに同意します。

6.2 Derived Benefit Locations

該当する場合、お客様が「IBM SaaS」に関する利益を享受しているとお客様が特定する所在地の税金が適用されます。IBM は、お客様が IBM に追加情報を提供する場合を除き、「IBM SaaS」の注文時に主要な Benefit Location 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、当該情報を最新状態に保ち、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。

6.3 セキュリティーの内容

本「IBM SaaS」は、IBM の「IBM SaaS」に関する「Data Security and Privacy Principles」(<http://www.ibm.com/cloud/data-security> 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「IBM SaaS」に関する「Data Security and Privacy Principles」が変更される場合であっても、それにより「IBM SaaS」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。

IBM はお客様にセキュリティー・インシデントの通知を行いますが、かかるインシデントの調査および解決はお客様の責任で行います。IBM は、未解決のインシデントが理由で「IBM SaaS」の障害が生じる場合、「IBM SaaS」を切り離して中断する権利を留保します。

IBM Cloud Integrated Analytics VPN Connectivity オファリングでは、IBM ネットワークとお客様のネットワークとの間のデータ伝送中に、コンテンツの暗号化を行います。「IBM SaaS」では、データ伝送を待

機中の静止時に、コンテンツを暗号化しません。お客様は、「IBM SaaS」に追加する前にコンテンツを暗号化する責任を負うものとします。

6.3.1 個人情報および規制対象データ

「マネージド・サービス・ゾーン」(定義は「別表 A」のとおり)で導入されるオファリングについて、当該オファリングの「サービス記述書」または「ご利用条件」には、個人情報および規制対象データの処理に関するセキュリティー要件の概要が記載されています。

「ホスト対象ゾーン」で導入されるオファリングについて、「IBM SaaS」は、個人情報またはセンシティブ個人情報などの規制対象コンテンツに関する特定のセキュリティー要件に則して設計されているものではありません。お客様は、お客様が「IBM SaaS」に関連して使用するコンテンツのタイプについて、本「IBM SaaS」がお客様のニーズを満たすものかどうか判断する責任を負います。

6.3.2 蓄積データの使用

IBM は、「IBM SaaS」に対する改善や拡張の IBM 社内における研究、テスト、および開発、またはよりカスタマイズされた有意義な経験をユーザーに提供する新サービスの開発を目的として、お客様による「IBM SaaS」の使用を監視することができます。この利用の際に、IBM は、お客様の許可ユーザーによる「IBM SaaS」の利用を反映する、集計された匿名形式の要約情報を蓄積して分析し、さらに、報告書、研究論文、分析、およびこれらの蓄積および分析から生じるその他の作業成果物(以下、総称して「蓄積データ」といいます。)を作成することができるものとします。IBM は、「蓄積データ」に対する権利を保持するものとします。

6.4 お客様の義務

6.4.1 IBM Cloud Integrated Analytics VPN Connectivity

- 「仮想プライベート・ネットワーク(以下「VPN」といいます。)」のアンケートに記入し、VPN 構成の開始日前に、レビュー用に IBM へ返送します。
- クライアント・エンタープライズ・ネットワーク、VPN およびセキュリティー要件について知識のある、技術に関する単一の連絡先を提供します。
- セキュリティーとネットワークを担当する管理者が、VPN 構成の構成および評価フェーズ中に、VPN セットアップを完了するために IBM と協力すべく対応できる状態にあることを確認します。
- VPN 用に使用されるクライアント・サイトにおける、ハードウェアおよびソフトウェアのあらゆる管理、保守、修正、構成およびテスト。
- 実装中に VPN 構成を検証するためのユーザー受け入れテスト。
- オンライン問題報告システム経由で VPN 構成に必要な変更を通知します。

別紙 A

1. IBM SaaS の概要

IBM Cloud Integrated Analytics Environment (CIAE) は、別途購入され、有効化された異なる「IBM SaaS」オファリング間およびセキュアなクライアント接続のためのオプション間のプライベートでネイティブな接続を提供する、導入モデルです。こうしたオファリングの2つの主要カテゴリーは以下のとおりです。

- IBM Analytics の完全に管理されたオファリング (例: dashDB Enterprise、BigInsights on Cloud、Cognos BI、その他)
- IBM Analytics のホスト対象オファリング (例: DB2 on Cloud、Master Data Management on Cloud、DataStage on Cloud)、および「ICIA サーバー」上に導入されたお客様が管理するソフトウェア、ホスト・ゾーンの「IBM SaaS」には以下が含まれます。

- インシデント通知
- 以下を除く、ハードウェア/インフラストラクチャー管理:
 - IBM Cloud Integrated Analytics Standard Security Appliance
 - IBM Cloud Integrated Analytics Enterprise Security Appliance
- IBM が管理するインフラストラクチャーに関する物理層の問題の通知および解決
- 設備セキュリティー、アクセス制御、および保守の記録
- メディアの廃棄および再利用

お客様は以下の使用許諾を購入しなければなりません。

- IBM Cloud Integrated Analytics Entitlement
- IBM Cloud Integrated Analytics VPN Connectivity、または IBM Cloud Integrated Analytics Standard Security Appliance、または IBM Cloud Integrated Analytics Enterprise Security Appliance。

「Data Security and Privacy Principles」文書において、および以下のオファリング記述書に別途記載されている場合を除き、「IBM SaaS」オファリングは Infrastructure as a Service (IaaS) オファリングとして分類されます。

1.1 IBM Cloud Integrated Analytics Environment

IBM Cloud Integrated Analytics Environment 以下の2つのゾーンで構成される IBM SoftLayer データ・センターで導入されます。

- a. CIAE ネイティブのマネージド・サービス (IBM が管理するサイト間の VPN を含みます。)、ならびに IBM Analytics が管理する SaaS オファリングが導入される場所である、「マネージド・サービス・ゾーン」。このゾーンは IBM が管理します。「Data Security and Privacy Principles」文書において、当該オファリングの「マネージド・サービス・ゾーン」の部分は Software as a Service (SaaS) オファリングとして分類されます。
- b. IBM Analytics がホストする SaaS オファリングが導入される場所である、「ホスト・ゾーン」。これらのシステムは以下に該当する場合があります。
 - DB2 on Cloud などのホスト対象オファリング
 - 下記の ICIA サーバー。
 - 「ホスト・ゾーン」には別途購入された、お客様が管理する IBM Cloud Integrated Analytics Standard Security Appliance または IBM Cloud Integrated Analytics Enterprise Security Appliance で、外部からのファイアウォールによって外部侵入から保護してもらうというオプションがあります。

1.2 IBM Cloud Integrated Analytics VPN Connectivity

IBM が管理するサイト間の VPN サービス。IBM Cloud Integrated Analytics Environment の使用が終了した時点で、IBM は各 VPN 接続を自動的に終了します。IBM Cloud Integrated Analytics VPN Connectivity サービスでは、Site-to-Site IPsec VPN テクノロジーを使用します。

1.3 IBM Cloud Integrated Analytics Standard Security Appliance

「ホスト・ゾーン」で導入され、お客様によって管理されるセキュリティー・アプライアンス。お客様が管理するサイト間の VPN またはお客様が管理するクライアントとサイト間の VPN を有効化するために、および公共のインターネットからの外部侵入からホスト・ゾーンをファイアウォールで保護するために、お客様により使用されます。

1.4 IBM Cloud Integrated Analytics Enterprise Security Appliance

「ホスト・ゾーン」で導入され、お客様によって管理されるセキュリティー・アプライアンスの冗長ペア。これは、お客様が管理するサイト間の VPN またはお客様が管理するクライアントとサイト間の VPN を有効化するために、および公共のインターネットからの外部侵入からホスト・ゾーンをファイアウォールで保護するために、使用できます。

1.5 ICIA サーバー

「マネージド・サービス」および「ホスト・ゾーン」におけるその他のアプリケーションへの高速の低遅延接続を必要とする、お客様が所有するアプリケーション向けに、ホスト・ゾーンで導入される IBM Cloud Integrated Analytics Environment サーバーは使用されます。

1.5.1 IBM Cloud Integrated Analytics Extra Small Server

お客様が管理する SoftLayer サーバー (1 パブリック仮想コア、4 GB RAM、25 GB SAN ディスクという最小仕様)。

1.5.2 IBM Cloud Integrated Analytics Small Server

お客様が管理する SoftLayer サーバー (4 プライベート仮想コア、16 GB RAM、100 GB SAN ディスクという最小仕様)。

1.5.3 IBM Cloud Integrated Analytics Medium Server

お客様が管理する SoftLayer サーバー (8 プライベート仮想コア、32 GB RAM、ディスク 1 100 GB SAN ディスク、ディスク 2 100 GB SAN ディスクという最小仕様)。

1.5.4 IBM Cloud Integrated Analytics Large Server

お客様が管理する IBM SoftLayer サーバー (16 プライベート仮想コア、64 GB RAM、ディスク 1 100 GB SAN ディスク、ディスク 2 100 GB SAN ディスクという最小仕様)。

1.5.5 IBM Cloud Integrated Analytics SAN Storage

SAN ストレージを、100 GB、250 GB または 500 GB の各増分単位で「ICIA サーバー」に追加できます。